Access control regulation in the health care sector

Beatriz Castro

Thesis in examensarbete, 30 HE credits
Examiner: Mauro Zamboni
Stockholm, Autumn term 2017
Abstract

This thesis is about access control in the health care sector. Access control is a function in IT-systems that allows authorized users to access data they have right to access, prevents unauthorized users from accessing data and prevents authorized users from disclosing data unlawfully. One of the pillars of access control is that a user only is authorized to access data that he or she needs to perform a task. This describes the principle of least privilege and its objective is to ensure data's confidentiality and integrity. In the health care sector where an increasing number of public and private stakeholders are processing sensitive data the application of this principle is essential to protect patients' privacy and confidence in the system. The lawmaker has incorporated the principle of least privilege in legal bodies such as the General Data Protection Regulation, Patient Data Act and the regulation of registers that allow processing of health data. This thesis examines how the lawmaker has incorporated the principle of least privilege to protect health data. Therefore, it examines access control regulation, in particular, requirements on management of access rights and log audits. The lawmaker has applied this principle through requirements on the system that should be incorporated by default and through requirements on management of access rights. The conclusion is that given that the tendency in health care, like in other sectors, is toward automation and more focus on self-care, the requirements should be directed more to systems than medical staff.
Table of contents

Abbreviations ........................................................................................................................................ 6
Definitions ............................................................................................................................................... 7
1. Introduction ......................................................................................................................................... 9
  1.1. Background ..................................................................................................................................... 9
  1.2. Purpose and questions ..................................................................................................................... 10
  1.3. Material and Method ..................................................................................................................... 11
  1.4. Delimitation .................................................................................................................................... 12
2. Chapter 1: Digitalization of health data and threats ............................................................................. 14
  2.1. What is health data? ........................................................................................................................ 14
  2.2. Digitalization of health data ............................................................................................................ 15
  2.3. Impact of the unauthorized access to health data .......................................................................... 17
      2.3.1.1. Damage to reputation ........................................................................................................... 18
      2.3.1.2. Discrimination ..................................................................................................................... 18
      2.3.1.3. Mistrust in the health care system ...................................................................................... 19
      2.3.1.4. Threats on the data subject’s safety and life ........................................................................ 20
      2.3.1.5. Impacts on freedom and autonomy ................................................................................. 20
3. Chapter 2: Information security regulation in the health care sector ..................................................... 23
  3.1. What is information security? .......................................................................................................... 23
  3.2. Legal requirements of information security in health data ............................................................. 24
  3.3. Challenges of health data in relation to information security ........................................................ 25
      3.3.1. Health data remains relevant .................................................................................................. 25
      3.3.2. Health data is processed by many controllers ........................................................................ 25
      3.3.3 Balancing access and confidentiality .................................................................................... 27
  3.4. Conclusion and remarks .................................................................................................................. 27
4. Chapter 3: Access control and the principle of least privilege ............................................................... 29
  4.1 Access control .................................................................................................................................... 29
      4.1.1. Definition ..................................................................................................................................... 29
      4.1.2. Access control in context ......................................................................................................... 30
  4.2. Principle of least privilege ............................................................................................................... 31
  4.3. Implementing access control in IT-systems ..................................................................................... 31
      4.3.1. Security policies, models, and methods .................................................................................. 31
  4.4. Conclusion and remarks .................................................................................................................. 33
5. Chapter 4: Access control and Principle of least privilege in health data protection regulation

5.1. Access control and Principle of least privilege in the GDPR

5.1.1. Material scope of the GDPR

5.1.2. Processing of sensitive data

5.1.3. Application of the Principle of least privilege in the GDPR

5.1.3.1. Purpose limitation

5.1.4. Appropriate Safeguards

5.1.5. Organizational and technical measures

5.1.6. Privacy by Design

5.1.7. Privacy by default

5.1.8. Data Protection Impact Assessment (DPIA)

5.2. Access control and application of the Principle of Least Privilege in the PDA

5.2.1. Scope of the PDA

5.2.2. Which data may be processed?

5.2.3. Who may access what?

5.2.3.1. Access to patient’s data within the same health care facility or process

5.2.3.1.1. Active choice

5.2.3.2. Access to patient data processed by another health care unit or process

5.2.3.3. Direct access by third parties

5.2.3.4. Patients’ rights in relation to processing of personal data

5.2.3.4.1. Patient’s consent

5.2.3.4.2. Patients’ right to block data

5.2.3.5. Patients’ right to access data

5.2.4. Implementation of access control in the PDA

5.2.4.1. Management of access rights

5.2.4.1.1. Needs and risk analysis

5.2.4.2. Compliance

5.3. Access control and application of principle of least privilege in register laws

5.3.1. Type of health data processed by registries

5.3.1.1. Statistics, follow-up and quality improvement of the operations

5.3.1.2. Research

5.3.2. Access control and implementation of the principle of least privilege

5.3.2.1. Access by the controller
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>PDA</td>
<td>Patient Data Act</td>
</tr>
<tr>
<td>POLP</td>
<td>Principle of Least Privilege</td>
</tr>
</tbody>
</table>
Definitions

For the purposes of this thesis the following definitions will apply.

Controller

The 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.

Data subject

An individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about.

Health care provider

Public authorities, county councils and municipalities when providing the health care services that are within the area responsibility of the public authority, county council or municipalities (public health care provider) and other legal person or private company that provides health care (private health care provider).

Health data

Data related to the physical or mental health of an individual, which reveals information about his or her health status;

Medical records

Collection of one or several care documents concerning a patient.

Patient

Every natural person, each time he or she contacts a health care
provider in matters related to his or her health status.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Receiver

Natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
1. Introduction

1.1. Background

The Swedish government has set out digitalization of health care services as one of the primary goals to achieve by 2025. The government states that digitalization in this sector will lead to an individual-centered health care system in which health care services will be more equal, efficient, accessible and secure. At the same time, continuing digitalization suggests that a broader range of users will have access to one of the most sensitive types of data, i.e., health data. Health data privacy breaches can have severe consequences for the right to privacy of individuals and affect the trust of patients in health care providers. Therefore, the lawmaker has focused not only on introducing requirements to protect health data but also on establishing requirements on IT-systems that process this type of sensitive data. These statutory provisions on IT-systems processing health related data aim to ensure its confidentiality, integrity, and anonymity. In this regard, effective mechanisms of access control are essential to protect patients’ data.

Access control is a central element of information security and is defined as a process by which use of system resources is regulated according to a security policy and is permitted only by authorized users according to that policy. The main objectives of access control are to prevent unauthorized users from gaining access to resources, to avoid legitimate users from accessing resources illegally and enabling authorized users to access resources in an authorized manner. To preserve information security, policies that control access to resources should abide by the so-called principle of least privilege. This principle implies that each user of a computer system should operate with the bare minimum rights necessary to function properly.

To ensure confidentiality, integrity, and anonymity of patients’ data, the lawmaker has transformed the principle of least privilege into a legal requirement. For instance, Chapter 4 section 2 of the Patient Data Act prescribes "A health care provider will determine the conditions under which the permission for access to patient-related data which is processed wholly or partly by automatic means. Such authorization must be limited to what is necessary

1 Socialdepartementet & SKL, Vision e-hälsa 2025, p.3.
2 Datainspektionen, 2017, pp.4 f.
5 Goodrich & Tamassia, 2014 p.16.
for the individual to fulfill their duties in health care”. Mechanisms that ensure compliance with access control regulations and policies are equally important. The importance of access control has become evident in several cases where medical staff has unlawfully accessed patients’ data. In June 2016 the Prosecutor’s Office indicted a physician accused of illegally accessing more than 400 medical records. The physician had illegitimately obtained administrator rights which he had later used to create several accounts from which he unlawfully accessed the medical records.7 Furthermore, The Data Protection Authority had already in 2013 issued a resolution identifying several weaknesses in the Karolinska University Hospital’s definition of unauthorized access and the mechanisms used to secure compliance through access control regulation.8

However, strict information security requirements may seem to contradict the objective of the government of facilitating access to patients’ data to make the health care provider more effective when treating a patient. As the official report of the state "Right information at the right time" indicated, various stakeholders within the health sector have expressed the need for a more permissive access regulation.9 On occasion, having all relevant information available when treating a patient may be a matter of life and death. On the other hand, having access to data which is not necessary to perform a task could lead to an increased risk of data privacy breaches.10 These issues are an example of how the digitalization of health care services has led to questions regarding the regulation of access to systems that process health data and of access control and the application of the principle of least privilege.

1.2. Purpose and questions

This thesis argues that the lawmaker has incorporated the principle of least privilege when regulating access control within the health care sector. This study analyzes the application of access control and the principle of least privilege on regulation regarding health data. Therefore, the questions addressed are the following: What is health data and what are the risks of its digitalization? What are the information security challenges regarding health data? What is access control and the principle of least privilege? Who can access data according to the principle of least privilege? Which are the legal requirements regarding access control and how do they embody the principle of least privilege?

7 Datainpektionen, 2017, p. 4 f.
8 Datainpektionen 920-2012 (2013-08-26).
10 Datainpektionen 1568-2014 (2014-12-08).
1.3. Material and Method

This thesis applies a dogmatic legal method. Therefore, as a first step, the relevant law as it exists needs to be determined, described and systemized. This method can also be used to criticize or critically review the result of the analysis of the current law, for example, through arguments that are based on the purpose of the law. Therefore, this thesis analyzes the traditional legal sources represented by General Data Protection Regulation, the Patient Data Act and regulation concerning registries that process health data. Other relevant laws such as the Publicity and Secrecy Act, the Penal Code and the Patient Safety Act are also analyzed in relation to the data protection regulation. The current Data Protection Directive and the Data Protection Act are analyzed when relevant to the interpretation of the GDPR. Furthermore, this thesis also examines applicable case law, resolutions from the Data Protection Authority, official reports of the Swedish government and government bills to interpret the legal bodies.

This study is framed within the field of legal informatics. Legal informatics is a branch of legal science that strives to go beyond the above described traditional, text-oriented analysis of valid law. This field may also be seen as a general theory of law focusing on the interaction of law and information technology. It is, therefore, interdisciplinary and complements the traditional legal perspectives from the fields of informatics. According to Peter Seipel, one of the main focuses of a general methodology of legal informatics is the development of terminology and concepts. This method involves adjusting, developing and bringing close legal and technical concepts; describing the IT environment in legally relevant ways; Investigation of overall frameworks and wholes and shaping the legal regulation according to the principle of “viable steering models”.

Therefore, this thesis complements traditional legal perspective with one of the fields of legal informatics, i.e., information security theory. This thesis will examine this interaction regarding access control and mainly analyze the influence of the principle of least privilege on access control regulation and how access control regulation affects IT security policies and the structure of IT-systems that process health data. Consequently, in addition to traditional legal sources, literature from the information security field and studies on health care providers’ IT-systems will also be analyzed.

11 Korling & Zamboni, 2013, p. 35.
12 Sandgren, 2015, p. 43.
13 Seipel 2004, p. 31-47.
1.4. Delimitation

As described in Chapter 1, health data is not just processed by health care providers but also by other controllers, including public authorities that provide other public services. This thesis analyzes mainly the access control regulation concerning the processing of health data by health care providers. The thesis also examines access control regulation regarding health data processed for statistical purposes or research. Therefore, this investigation does not analyze the processing of the health data for the provision of social security or social services.

Access control refers not only to a system function that regulates access to data between a user and a database, but also programs, processes, or other systems’ access to data. Unlike “user to system” access control, the lawmaker indirectly regulates access control regarding programs, processes, or other systems’ access through technical rules such as information security standards. Therefore, this thesis only analyzes access control from a user to system perspective.

This thesis focuses mainly on the administration of privileges or access rights in the context of access control. The access control function determines whether a user is authorized to access specific data. Granting access requires that it is possible to ensure that the user is the natural person who has the right to access the data in question. The system provides that a user is related to a natural person through different authentication methods. The regulation concerning health data, and in particular the PDA, establishes requirements regarding the authentication methods that the health care provider should incorporate into the system to access patient data. Even though authentication methods are central to guarantee patient’s data confidentiality and integrity, the regulation on authentication is extensive. Hence, authentication is excluded from this study.

1.5. Outline

The first chapter aims to emphasize the importance of the topic of this thesis. Therefore, it answers the question: What is health data and what are the risks of its digitalization? This chapter defines health data according to the European law and outlines the characteristics of health data that make it the subject of special protection as sensitive data. This chapter also analyzes the consequences of security violations that lead to the accidental or unlawful
disclosure of health data. Finally, this chapter describes the objective of information security in the health care sector and how the lawmaker has translated these objectives into regulations.

The second chapter brings concepts and terminology from the legal and the information security theory field together to examine how information security applies to processing of health data and what are the challenges of its application.

The third chapter examines one of the pillars of information security: access control. Moreover, this chapter examines the principle of least privilege within the frame of access control and explain who, according to the principle of least privilege, should be authorized to access data.

Finally, the third chapter answers the question: Which are the legal requirements regarding access control and how do they embody the principle of least privilege? The chapter describes, in general terms, which data the controller may legally process and who can access which health data. Additionally, this chapter analyzes the access control regulation, particularly the management of access rights and audits of logs. This analysis structure is applied to the primary relevant legal bodies, i.e., the GDPR, the PDA and the regulation concerning registries that process health data.
2. Chapter 1: Digitalization of health data and threats

2.1. What is health data?

Health data was firstly defined in the EU as “all personal data concerning the health of an individual”.\(^{14}\) Furthermore, “It refers also to data which have a clear and close link with health as well as to genetic data”.\(^{15}\) According to this definition what defines health data is its content. Therefore, the controller or the context in which the health care is provided is not relevant to classify data as health data. The controller could be a health care provider or not, and the context might be other than a patient requiring medical attention. Secondly, health data is personal data. This concept of health data is broad since it also includes the concept of “genetic data”.

The Data Protection Directive stipulates that ‘data concerning health’ was sensitive data,\(^{16}\) but did not define the concept. The GDPR classified ‘data concerning health’ as sensitive data. However, unlike the Directive it incorporated a definition of ‘data concerning health’. ‘Data concerning health’ is, according to the GDPR, sensitive data.\(^{17}\) The GDPR defines “data concerning health” as “personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status”.\(^{18}\)

In addition, according to Recital 35 GDPR “Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; 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

\(^{14}\) Principle 1, Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data (Adopted by the Committee of Ministers on 1997-02-13 at the 584th Meeting of The Ministers’ Deputies).

\(^{15}\) Ibid.

\(^{16}\) Article 8.1 Data Protection Directive.

\(^{17}\) Article 9.1 GDPR.

\(^{18}\) Article 4.15 GDPR.
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.’”

Unlike the definition of the Committee of Ministers the GDPR did not include genetic data in the definition of health data. The GDPR defines Genetic data as “personal data relating to the “inherited or acquired genetic characteristics of a person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample”.¹⁹ According to this definition, genetic data may be classified as health data if it provides information about the health of a natural person. In other words, genetic data that only provides information about a physical person’s physiology is not considered data concerning health.

2.2. Digitalization of health data

Medical records during the early 90’s was still mostly in paper format. But the digitalization in the Swedish health care system has evolved rapidly since then. Health care providers, who at that time were mainly counties and municipality, initiated digitalization. The year 2007, when the PDL was proposed by government 97% of the primary health care system used digital medical records, hospitals used digital means to document 81% of the information and 83% of the information was documented using an IT-system in the psychiatric care sector. This digitalization entailed faster access to medical records.²⁰

As the state allowed private actors in the health care sector, the number of health care providers grew exponentially. The need to access data regarding patients that was processed by another health care provider to pursue efficiency and higher care quality led the Government to adopt the regulation that allows collaborative medical records. Health providers connected to this system can access the patient’s medical records regardless of where the information has been collected. Nowadays, Sweden has vastly adopted ICT in their health care system ranging from fully digitalized patient health records and e-prescriptions to different types of clinical decision support systems for different aspects of care.²¹ Robots that perform surgeries and diagnose diseases are seen today as tools, and it is realistic to believe

---

¹⁹ Article 4.13 GDPR.
²¹ SOU 2016:2 p 305.
that the health care sector will become more effective and the cost will be lowered replacing employees for computers and robots.\textsuperscript{22}

The patients and the information given to them will also play an important role in the digitalization of the health care sector. The Government has expressed that one of the objectives of digitalization is to simplify access for patients to the information stored about them. The digitalization also leads to decreasing medical staff and costs for establishments. If one in five Swedes chose to replace primary care by app consultation the state would save 1.2 billion kr a year.\textsuperscript{23} This would be possible through online medical services, such as web pages that allow to book medical consultation and receive all the information regarding a patient’s health.\textsuperscript{24} Another example are apps that allow patients to get online primary care. If personal consultation is not necessary the physician may issue a prescription that the patient can order online and receive at home even the same day.\textsuperscript{25}

Also, individuals voluntarily share data concerning their health to private companies that provide health-related services. An example of the latter are apps and devices that monitor physical activity, heart rate, nutrition, menstrual cycles, among other data. This, in combination with the data provided by the health sector, might provide a detailed description about a person’s health. The big data related to health might lead to predictive modelling.\textsuperscript{26} Within the health industry, the use of technology based on data and modelling practices is helping medical practitioners diagnose and treat illnesses.\textsuperscript{27}

Predictive modelling technologies are being used are so called smart houses. The concept of smart home technologies is being explored especially for the future of healthcare and well-being of older adults, people with disabilities but also for the general population overall. Smart homes enable patient self-treatment and monitoring by using simple devices, which

\begin{footnotesize}
\begin{enumerate}
\item SOU 2016:2 p. 146 ff.
\item PWC, 2015, p. 5.
\item Hälsa för mig is a digital service created by the E-Health authority. The service aimed to provide platform containing health data that companies, and organizations could access through apps. The patient would access his or her health data, compiled by health providers, and even generate own data E-Health Authority, https://www.halsaformig.se/, last accessed 2017-08-08. The DPA considered that the initiative was illegal according to the data protection regulation, and especially in the light of the enter into force of the GDPR.
\item KRY and Min Doktor are tho of the most utilized apps in this field. Online pharmacies like apotea.se is one of the most popular just online pharmacies that offer this type of service. Datainspectenon, 2276-2016 (2017-04-21).
\item Predictive modelling is a technology based on applies statistics, mathematics machine learning an artificial intelligence that use algorithms to analyze big data collections, and identify patterns that are invisible to human beings. Greenstein, 2017, p. 22 ff.
\item Memorial Sloan Kettering Cancer Center.
\end{enumerate}
\end{footnotesize}
provide standardized outputs for specific physiological conditions, intelligent applications or software capable of analyzing and processing body signals, sensor-integrated smart devices, wearable sensors, and other devices exclusively manufactured for the purpose of body signal monitoring and processing.\textsuperscript{28} Smart homes imply not only collecting big amounts of data (big data) but also finding patterns in order to detect current or predict future medical issues.

2.3. Impact of the unauthorized access to health data

Recital 75 GDPR warns about the risk that may result from processing personal data: ‘The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where (…) the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.”

This section describes different issues that arise when unauthorized users access health data or unlawfully disclose health data. The consequences of unauthorized access or disclosure depend on the content of the data leaked and other circumstances. Moreover, the consequences will depend on the data subject's perception and who receives the information.\textsuperscript{29}

How the victim might experience the consequences of unauthorized users having access to their patient data also varies. Some patients fear effects on their reputation\textsuperscript{30}; meanwhile, others might interrupt their treatments.

\textsuperscript{28} Athavale.
\textsuperscript{29} Vårdanalys, s. 57 ff.
\textsuperscript{30} SOU 2014:45, p. 20 och Datainspektionen 2016c, p.3
2.3.1.1. Damage to reputation

The unauthorized disclosure of patient data usually also leads to an unwanted exposure of that individual’s private life. Hence, the beliefs and opinions held by others regarding the data subject might be affected. The data subject’s sole belief that his or her reputation has been damaged constitutes harm \textit{per se}. The damage to an individual’s reputation may depend on the data disclosed, the data subject’s perception and who receives the information. Data regarding mental and sexual health are considered as the most sensitive data and its unauthorized disclosure may lead, in most cases, to a greater harm of reputation than, e.g. blood type.

Harm of reputation can be a strong reason for concern when relatives access some types of data, such as those related to abortions or the use of contraceptives. For the same reason, other individuals might be concerned about medical staff accessing and reading medical records of patients they are close to, for example, neighbors and relatives.\footnote{Vårdanalys, p. 68.}

2.3.1.2. Discrimination

Going one step further, unauthorized disclosure data regarding mental health and sexual health is more likely to lead to discrimination, more than any other type of data.\footnote{Ibid.} One study has shown that there is an impending risk that individuals with mental illnesses or issues noted in their medical records might receive lower quality health care services than individuals without these types of notations. This study also showed that physicians avoid registering certain sensitive data about patients in the medical record so that the patient’s health care is not affected.\footnote{Folkhälsomyndigheten, 2015, p. 30 ff. \& Oldenfors.}

Furthermore, data subjects may be discriminated by employers, banks, and insurance companies. In the case of banks and insurance policies the access to health data might lead to denial of loans and insurances or increasing fees. An example that illustrates the above is the case of an insurance company that denied health insurance policy to a woman and her
daughter. The insurance company claimed that parents whose children received public health support, statistically worked less than average.\(^{34}\)

In the case of employers, access to health data might condition the data subject’s employment possibilities. For example, medical workers might fear that they will not be employed if data regarding mental health issues is disclosed.\(^{35}\) Another example is the refusal to employ the data subject because she is pregnant or he or she has a medical history related to illnesses or issues that might affect the employees working capacity.

Processing of large quantity of data, so called big data, might also lead to the categorization and classification of people regarding, e.g., their genetic markers, heart rate, eating habits, sexual health, etc. that are then compared to statistics related to a group or category.\(^{36}\) This could, for example, be done through profiling, which is defined as any form of automated processing of personal data leading to the use of it to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.\(^{37}\)

2.3.1.3. Mistrust in the health care system

The reaction of data subjects to unauthorized disclosure of health data varies. In some cases, if the information has been disclosed by a health care provider, the data subject will lose confidence in the health care system. An example of the latter is the case where a psychiatric health care provider sent an e-mail to almost 2000 people in which the e-mail address of all the recipients was visible. As a result, a lot of patients worsened significantly, and some of them even interrupted their treatment.\(^{38}\)

\(^{34}\) RH 2014:9.

\(^{35}\) A health care worker that requested the destruction medical records concerning mental health to the Health and Social Care Inspectorate claimed that she wanted to apply for a job in health care. Even though she did not explicitly state it in the claim, it was apparent that she feared that her possibilities of being employed would be affected by the content of her medical record. Health and Social Care Inspectorate and the Administrative Court denied her request due to the lack of legal grounds for the destruction of her records. Förvaltningsrätten i Stockholm dom 2016-10-28 (14576-16) and Inspektionen för Vård och Omsorg 33230/2015 (2016-06-30).

\(^{36}\) Lupton, 2012, p. 234 f.

\(^{37}\) Article 4.4 GDPR.

\(^{38}\) Malm, 2015.
2.3.1.4. Threats on the data subject’s safety and life

Disclosure of very sensitive data such as information about sexual health might lead to persecution and threat of the data subject’s life. This might be the case of data that reveal sexual preferences or gender or abortion-related data. In other cases, the disclosure of personal data such as name or address might have a significant impact. For example, this is the case of individuals with protected identity or address.\(^39\)

Besides patients discontinuing their treatments, patients may also avoid providing accurate and complete information about their health, fearing that the information will reach unauthorized users. At the same time, this may impact on the quality of the health care service they will receive.\(^40\)

2.3.1.5. Impacts on freedom and autonomy

Health data falling into the wrong hands might even have severe consequences on an individual’s freedom. Health data may be used to control individuals’ lives and decisions. An example of this is the case of a physician who was convicted for committing 177 data breaches during 2012 when accessing unauthorized the medical records of 20 women. Regarding 16 of these patients he sought information regarding e.g., contacts with mental health care, sexually transmitted diseases tests and contacts with women’s clinics. Based on the testimony provided by some of the victims, the Courts of Appeal of Scania and Blekinge concluded that the motive behind these searches was the existence of a culture among some Afghans in Malmö that entailed that they should control unmarried women.\(^41\)

Stanley Greenstein states that the use of predictive modelling in health would be beneficial from the societal perspective, as the ability to cure illnesses would increase. At the same time, modelling technology could potentially erode an individual’s privacy and autonomy. Data reveals how to predict a data subjects’ behavior from a big quantity of data. The health of individuals relates to their life choices and environment, and therefore data captures connections predictive of health based on type of neighborhood and household characteristics, your job satisfaction relates to your salary, evaluations and promotions, among others.\(^42\)

\(^39\) Vårdanalys, p. 69.  
\(^40\) Folkhälsomyndigheten 2015, p. 30 ff.  
\(^41\) Kammarrätten i Stockholm dom 2015-12-02 nr 7632-15.  
\(^42\) Siegel, 2013, p. 79.
Based on certain health indicators, health care be provided in such a way that individuals can reach these standards, leaving no room for autonomy.

2.4. Conclusion and remarks

The concept of health data has expanded since the first definition by the Committee of ministers. The GDPR specifies, for example, that data concerning health comprises both physical and mental health. The GDPR also emphasizes that this concept also encompasses the information processed by health care services that reveals information about an individual’s health. The latter could be the case of information regarding an individual seeking medical attention. The information might not exactly reveal that the individual in question has a certain diagnose, but it might suggest that he or she has a certain disease or injury. The expansion of the concept is a consequence of the expansion of the digitalization of data concerning health.

Digitalization of health data is increasing. It started with medical records within the same health care facility, to access allowed to by health care providers, IT-services for booking medical consultation, and then providing other services as allowing the patient to access his or her own health data. At the same time, more stakeholders are collecting more health data. Apps connected to mobile devices with sensors collect live data such as blood pressure and physical activity. The digitalization of health data simplifies and increases transparency in the health care provider-patient relationship. Providing the data subject with more information concerning his or her health decreases costs and allows the data subject to make informed decisions.

Processing large amounts of data leads to increasing security risks. The prospect of users unlawfully accessing and eventually disclosing extremely sensitive data increases. Unlawful access and disclosure may have impacts not merely on the data subject but on society as a whole. Impacts on the data subject may depend on the type of data disclosed, the receiver, the perception of the data subject and other circumstances. Harm of the reputation of the data subject, loss of trust towards the health care system and discrimination are among the ‘milder’ impacts of disclosing health data while threats to the patient’s safety and life are among the most severe consequences. The processing of big data may lead to categorization and division

---

43 A Health indicator is a characteristic of an individual, population, or environment which is subject to measurement (directly or indirectly) and can be used to describe one or more aspects of the health of an individual or population (quality, quantity and time). WHO, 1998, p. 9.
of individuals into groups in relation to health indicators. Predictive modelling might even lead to the standardization of health and loss of individual’s autonomy regarding their health. Therefore, regulation of security measures to protect health data is essential to avoid the above described impacts on individuals, the health care system’s credibility and those on society as a whole.
Chapter 2: Information security regulation in the health care sector

3.1. What is information security?

Information or computer security is “the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications)”\(^{44}\). The definition introduces three key objectives that are at the heart of computer security, i.e. confidentiality, integrity and availability. These three concepts are often referred to as the CIA triad\(^{45}\) This definition of information security and its components are common to both the legal field and computer science field.

The first concept, confidentiality, implies preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information\(^{46}\). Confidentiality covers two related concepts: data confidentiality and privacy. Data confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals. Privacy ensures that individuals control or influence what information related to them may be processed and by whom and to whom that information might be disclosed. Applied to health data, confidentiality implies that only authorized users will have access to health data. Who an authorized user is can be defined by law or information security policies.

The second concept, integrity, aims to ensure the nonreputation of information (that the information cannot be questioned) and authenticity. A loss of integrity is the unauthorized modification or destruction of information\(^{47}\). Integrity comprises two concepts, i.e. data integrity and system integrity. Data integrity ensures that information and programs are changed only in a specific and authorized manner. System integrity ensures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system\(^{48}\). Applied to health data, integrity entails that authorized and unauthorized users who have access to the data are not able to alter or destroy...

\(^{44}\) Krutz, Ronald L. & Dean Vines, p. 624.
\(^{45}\) Goodrich, M. & Tamassia, 2014
\(^{46}\) FIPS, 2004, p. 2.
\(^{47}\) Ibid.
\(^{48}\) Ibid.
the data in an unauthorized manner, and, therefore, the medical staff can rely on the medical data that is available in the system.

The third concept, availability, ensures that systems work promptly, and service is not denied to authorized users. It implies guaranteeing timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. Applied to health data, availability entails that medical staff has relevant medical information available when needed to take a medical decision, such as diagnoses and treatment.

### 3.2. Legal requirements of information security in health data

The GDPR regulates who can process what and under which circumstances. Moreover, the GDPR requires the controller to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing (principle of integrity and confidentiality).

Recital 49 GDPR requires that the processing of personal data is limited to the ‘strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data (...). This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.’

Applied to the health care sector the controller also must guarantee patients’ right to privacy, self-determination and participation in his or her own health care.

Furthermore, the DPA also requires patients’ data to be processed so the patients’ and other registered individuals’ privacy is respected. Documented data shall be managed and kept so that unauthorized persons cannot access them.

---

49 Certification Magazine.
50 Article 5.1.f GDPR.
51 Chapter 1 section 1 PDA.
52 Chapter 1 section 2 PDA.
The medical records regulation states that the health care provider is responsible for implementing processes and routines that ensure the security of the personal data processed. These processes and routines should be part of a management system that ensures that 1) documented personal data are accessible and useful to an authorized user (availability), 2) personal data is not altered (integrity), 3) unauthorized users should not access personal data (confidentiality) and 4) processing in systems that are wholly or partly automatically processed personal data can be traced to a user (traceability).

3.3. Challenges of health data in relation to information security

The digitalization of the health care system implies the extensive processing of individuals’ health data. This type of data is especially sensitive due to some of its characteristics. Below we explain some of them.

3.3.1. Health data remains relevant

Unlike credit card numbers, passwords or even ID-numbers, there is no means to change some health data neither by the passing of time nor by intervention of the patient or others. Therefore, once an unauthorized person has accessed and disclosed another person’s DNA or blood type, the data will remain relevant maybe even after the person’s death. This circumstance also adds to the importance of information security. Even though data is encrypted, an unauthorized user that accesses the data might store it until the day technology that allows the decryption is available. Past medical issues or illnesses may also remain relevant if compared to statistics about individuals who have suffered a certain issue or illness.

3.3.2. Health data is processed by many controllers

In Sweden, the number of health care providers has increased since the enforcement of the Patient Act in 2015 and the liberalization of the pharmacy market in 2009. In addition, stakeholders who do not provide health care services has also increased. This is better described through the following example. A patient seeks medical attention in a primary care facility and provides information concerning his or her symptoms to the primary health care

---

53 Chapter 3 section 2 Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

54 This act gave patients the right to choose public primary care provider and outpatient care (private or public), which lead to an increase in private actors.
The primary care provider is required to send data to several public authorities that are responsible for registries that process health data. Public authorities and researchers might have access to the data for statistical studies or research purposes. Part of this medical data, such as prescriptions, will be available in a system that pharmacies can access so that the patient can order prescribed medication. The data might also be available to supervising authorities, for example the Health and Social Care Inspectorate, if the health care provider decides to denounce irregularities in the provision of health care. The patient, him/herself, might also voluntarily provide health data to private companies that offer health care services, for example, Google or Apple, through health apps or devices. This data may be collected in the same system platform, as intended by the E-health authority. See example of information flow below.

![Diagram of data flow](image_url)

**Figure 1. Source:** Translation of figure 1 in Vårdanalys, p. 28.

---

55 Chapter 3 PDA.
56 See for example section 6, lagen (1998:543) om hälsodatatable and Chapter 5 PDA.
57 Chapter 3 section 3 Patientsäkerhetslagen (2010:659) and Inspektionen för vård och omsorgs föreskrifter (HSLF-FS 2017:41) om anmälan av händelser som har medfört eller hade kunnat medföra en allvarlig vårdskada (lex Maria).
58 A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed. In personal computing, a platform is the basic hardware (computer) and software (operating system) on which software applications can be run.
The more users have access to data, the more vulnerable a system becomes. More users imply more targets for different methods to unlawfully accessing sensitive data, such as social engineering, i.e. techniques involving the use of human insiders to circumvent computer security solutions.\textsuperscript{59} More users also entail an increased in risk for some of them not following information security policies.

3.3.3 Balancing access and confidentiality

The gathering of information is not enough to improve the quality of health care. The information regarding a patient or several patients must be available for the controller to have access to this information. The digitalization may lead to prevent illnesses and medical issues if systems and medical staff have access to information about patients, their medical history, risk factors and available treatment guidelines. Effective processing of data might result in earlier diagnoses of illnesses and earlier treatment.\textsuperscript{60} Therefore, a Swedish Government Official Report manifested the need of eliminating legal and organizational barriers to processing personal data in the health care system. The Report warned for an increase in the risk of patients receiving less safer treatments or treatments of lower quality due to the lack of access to right information in the right time and proposed the creation of a new Health Care Data Act, which would replace the PDA.\textsuperscript{61} The purpose of this law is promoting a processing of data that leads to good quality, patient safety and cost efficiency.\textsuperscript{62} At the same time, as the DPA has indicated, effectivization of data processing and incorporation of new technologies if often conveyed as increased risks for privacy.\textsuperscript{63}

3.4. Conclusion and remarks

In principle, systems that process health data must comply with the same requirements as other systems that process other types of data. Nevertheless, ensuring availability, confidentiality and integrity in relation to health data might have more significance in comparison to other data. For example, not having access to a patient’s medical history available in an emergency, having access to unlawfully altered information or unlawfully

\textsuperscript{59} Goodrich, M. & Tamassia, 2014, p. 43. Examples of social engineering are phishing, pretexting, baiting, quid pro quid and tailgating.

\textsuperscript{60} SOU 2014:23 p. 66.

\textsuperscript{61} SOU 2014:23 p. 29.

\textsuperscript{62} SOU 2014:23 p. 131.

\textsuperscript{63} Datainspektionen 1568-2014 (2014-12-08).
disclosing health data might lead to severe consequences for the affected individual, the health care provider and society.64

Health data has characteristics that makes it especially vulnerable. Some types of health data, such as genetic data remain relevant. Thus, this type of data does not lose value, on the contrary, this data will likely gain value as medical sciences develop. As mentioned in Chapter 1, several actors, for instance, banks, insurance companies and employers might be interested in collecting this data. Health data is also processed by several actors, public and private. More users being processed leads to more targets for hackers and an increasing possibility that one or more controllers might not have adequate protection measures.

The digitalization of health care may result in a more effective health care, reduction of costs and more accurate diagnoses and treatments. Access to data concerning patients is essential to implement improvements in health care through digitalization. Nevertheless, an excessively liberal approach of access to health data may result in a weakening in the security of the information and therefore jeopardize its confidentiality as pointed out by the DPA in the proposition. At the same time, there is an increased risk of breaches of data privacy if the systems do not guarantee data confidentiality and integrity.

Breaches of data privacy might lead to severe harm on the data subject’s integrity as well as on society. Finding a balance between availability and confidentiality is a subject of discussion and no conclusion is reached so far.

---

64 See Chapter 1.
**Chapter 3: Access control and the principle of least privilege**

4.1 Access control

4.1.1. Definition

Access control is defined as a process by which the use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.\(^{65}\)

In other words, access control is a security requirement that implies limiting the information system to authorized users, processes acting on behalf of authorized users (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.\(^{66}\) In the context of health data, access control implies that systems that contain health data should only permit access to authorized users, e.g., the medical staff that has a patient relationship to the data subject.

The main objective of access control, as of computer security, is to prevent unauthorized users from gaining access to resources, to prevent legitimate users from accessing resources in an unauthorized manner, and to enable legitimate users to access resources in an authorized manner.\(^{67}\) Applied to health data, this implies that the system should prevent that, e.g., non-medical staff access medical records. It also implies that authorized medical staff do not access data regarding a patient for other purposes (for example, gossiping) than providing health care and that treating medical staff should access the relevant information regarding the patient they are treating.

The general rule is that it is the controller who decides, through a security policy, which users may have access to reach specific system resources and the type of access that is permitted, called privileges or access rights. However, in the case of health data, the lawmaker has established requirements on an information security policy. Therefore, this policy should contain rules that apply to access control. Furthermore, the lawmaker has regulated who may have access to each specific health data. In consequence, access control regarding systems

---

\(^{65}\) IETF 2007.

\(^{66}\) Stallings & Brown, 2015, p. 114.

\(^{67}\) Ibid.
that process health data is not only dependent on information security policy but also to legal requirements.

4.1.2. Access control in context

An access control mechanism mediates between a user (or process executing on behalf of a user) and system resources, such as applications, operating systems, files, and databases. See figure below.

Figure 2. Source: Based on Stallings & Brown, 2015, p. 115.

The system must first authenticate a user requesting access. Authentication implies the verification that the credentials of the user are valid. The authentication function determines whether the user is permitted to access the system. Afterwards, the access control function determines if the specifically requested access by this user is permitted. A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user to answer the question if the specific user can access the specific resource. This function determines who is trusted for a given purpose. The access control function consults this database to determine whether to grant access. If the user has the right to access the system resources, he or she is authorized, i.e., has been granted a right or permission to access a system or entity.

Finally, an auditing function keeps a record of user accesses to system resources. Auditing implies an independent review and examination of system records and activities to test for adequacy of system controls and operational procedures, to detect breaches in security and to
recommend any indicated changes in control, policy, and procedures. In the case of health data, breaches in the security might lead to criminal charges.

4.2. Principle of least privilege

The principle of least privilege states that the security policy or regulation should give the subject only those privileges (or access rights) that it needs to complete its task.68 The application of this principle helps reduce the vulnerability of the system by eliminating unnecessary privileges that can result in network exploits or system compromises.

If this principle is enforced, the damage caused by the compromise of a particular user account is minimized. The military concept of need-to-know information is an example of the application of this principle. When the principle of least privilege is ignored, then extra damage is possible from security breaches.69 For instance, an unauthorized using an authorized user’s account will have access to all the system resources if the access rights of the authorized user is not limited to what he or she needs to fulfill his or her tasks.

4.3. Implementing access control in IT-systems

The development of an access control system requires the definition of security policies used to verify whether an access request is to be granted or denied. A policy is then formalized through a security model and is enforced by an access control mechanism.70 Note that this policy should incorporate the legal requirements regarding access control.

All models assume that there are data managers, data owners, or system administrators who are defining the access control specifications. The intent is that these users should be restricting access to those who have a need to access and modify the information in question. That is, they should be applying the principle of least privilege.71

4.3.1. Security policies, models, and methods72

The security policy defines the rules according to which access control is regulated. The term policy is also used to refer to documents that describe the authorizations and access

---

68 Bishop, 2003, p. 20.
restrictions to be enforced by the controller and the specific users that are not yet enforced, but planned. In this context, a security model should provide a formal presentation of the access control policy which is currently being enforced. Security models are usually written to describe the properties of an access control system. Finally, a security mechanism defines the software and hardware that are used to implement the controls imposed by the policy and formally stated in the model. The access control mechanism must work as a reference monitor, that is, a trusted component intercepting every request to the system.

An access control policy, which can be embodied in an authorization database, dictates which type of access is permitted, under what circumstances, and by whom. Access control policies are grouped into the following categories which are not mutually exclusive:

**Discretionary access control (DAC):** Discretionary access control is “a means of restricting access to objects based on the identity of subjects and groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).”\(^{73}\) In other words, users can be given the ability to pass on their privileges to other users, where granting and revocation of privileges is regulated by an administrative policy.\(^{74}\)

**Mandatory access control (MAC):** Access control policy based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is called mandatory because, unlike DAC, an entity that has clearance to access a resource may not, just by its volition, enable another entity to access that resource.

**Role-based access control (RBAC):** Access control based on the roles that users have within the system and on rules stating which accesses are allowed to users given roles. Essentially, role based policies require the identification of roles in the system, where a role can be defined as a set of actions and responsibilities associated with a particular working activity. The role can be widely scoped, reflecting a user’s job title (e.g., physician), or it can be more specific, reflecting, for example, a task that the user needs to perform (e.g., heart surgery).

\(^{73}\) US Department of Defense, 1985, p. 11 ff.
\(^{74}\) ECS, 2014 p. 357.
Then, instead of specifying all the accesses each user is allowed to execute, access authorizations on objects are specified for roles. Users are then given authorizations to adopt roles that are tied to access rights. In general, a user can take on different roles on different occasions.  

4.4. Conclusion and remarks

Access control constitutes a fundamental part of information security. It ensures that authorized users can lawfully access data (availability) and prevents users from unlawfully accessing or modifying data (confidentiality and integrity). Who has access to which data, i.e. access rights or privileges, will be determined by a security policy. The management of access rights might also be determined by law, as we will analyze in the following Chapter. Furthermore, the sole function of access control is not sufficient to ensure information security. The function presupposes the existence of a secure authentication method, that is capable to ensure that the user is the natural person who is entitled to access the data. Access to data must be made traceable through logs so that the controller is able to audit and detect unauthorized access. Furthermore, compliance of the security policy must be followed-up on to improve compliance and prevent further unauthorized access.

When determining access rights, the controller or lawmaker should apply the principle of least privilege to avoid security breaches. In the health sector, these breaches may have severe consequences on individuals and society. These breaches might not only come from outside an organization but also from inside, as in the case of so called ‘gossip reading’ of medical records. Thus, it is essential that users only have access to the information they need to fulfill their tasks. Regarding systems that process health data, the principle of least privilege has a central role in protecting the data subject’s integrity.

The access control policy is what will define the models and the mechanisms for access control. The role-based access control is the policy that most reflects the principles of least privilege as it bases access rights on roles that a person might have in an organization. This role is related to a set of tasks which have corresponding access rights. Albeit determining how detailed these roles and tasks should be defined when determining accessing rights is not clear. Access control may be ineffective if in too general terms.

75 Ibid.
5. Chapter 4: Access control and Principle of least privilege in health data protection regulation

5.1. Access control and Principle of least privilege in the GDPR

The GDPR is a European regulation and is, therefore, superior to all national laws that are analyzed in this chapter. Thus, the analysis in this section is applicable to the processing of data according to the PDA and register laws.

5.1.1. Material scope of the GDPR

The GDPR applies to personal data. According to article 4.1 GDPR personal data is “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, 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”.

5.1.2. Processing of sensitive data

Health data has been previously regulated by section 18 Data Protection Act. Health data must be lawfully processed. Furthermore, it is classified as “sensitive data”. Sensitive data is all personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and their processing convey significant risk. In principle, it is forbidden to process such personal data to including health data and genetic data. However, there are exceptions. Some of these exceptions require the existence of national laws that allow the processing of the data. Note that, following that, the requirements established for every exception are only a minimum standard and the Member States are allowed to maintain or establish further requirements to process sensitive data.

76 The Swedish implementation of the Data Protection Directive in section 18 § 2 Personuppgiftslag (1998:204) has been criticized limiting the requirements to professional secrecy when processing health data. The requirement on professional secrecy should be additional to the requirements of certain purposes to process sensitive data according to section 10 Personuppgiftslag (1998:204). SOU 2006:82 p. 175 and Rynning, 2003, p. 112.
77 Article 6 GDPR.
78 Article 9.1. GDPR. The same provision is found in article 8.1 Data Protection Directive.
79 European Patients Forum.
80 See articles 9.2 a, b, g, h, i and j GDPR. The requirement of secrecy also refers to the national law.
The data subject gives explicit and unambiguous consent to the use of their data for one or more specified purposes.\textsuperscript{81} It is the controllers’ responsibility to show that the patient or data subject has given his or her consent.\textsuperscript{82} Therefore, the data subject has to make “affirmative action”\textsuperscript{83} to clearly show that he or she agrees with his or her data being processed. An example of consent is the informed consent forms through which clinical trials often ask patients for their consent regarding the use of their data.\textsuperscript{84}

The data of the data subject is manifestly made public by the data subject himself or herself.\textsuperscript{85} If patients make their health data public, the data is no longer particularly protected as sensitive data since it means the data subject has agreed to it being used by third parties. The fact that the data subject has made the information public is interpreted as he or she having consented that third parties have access to the public data. The interpretation of the term “manifestly public” may differ from one Member State to another.

For health care purposes.\textsuperscript{86} The controller may process health data of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care or treatment, as well as the management of health or social care systems and services.\textsuperscript{87} In these cases, personal data can only be collected, used or shared by a person subject to professional secrecy.\textsuperscript{88} When processing health data for health care purposes, the controller does not need the data subject’s consent.

For public interest in the area of public health.\textsuperscript{89} This ground refers to, among other cases, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products or medical devices. In this case, it is also required that the data is subject to safeguards, especially professional secrecy.

\textsuperscript{81} Article 9.2 a) GDPR.
\textsuperscript{82} Article 7 GDPR.
\textsuperscript{83} European Patients Forum.
\textsuperscript{84} Ibid.
\textsuperscript{85} Article 9.2 c) GDPR.
\textsuperscript{86} Article 9.2 h) GDPR.
\textsuperscript{87} The Data Protection Report’s proposition of ‘Data Protection Act’ states in chapter 3 section 5 that the data can be processed if it is necessary for preventive health care and occupational medicine, assessment of an employees working capacity, medical diagnoses, provision of health care or treatment, social services or management of social services, health care services and their system. The processing if allowed of the controller complies with the requirement of secrecy in 9.3 GDPR. SOU 2017:39 p. 41.
\textsuperscript{88} Article 9.3 GDPR.
\textsuperscript{89} Article 9.2 i) GDPR.
To carry out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law:90 This processing of health data is often necessary so that the data subject can obtain, e.g., social benefits. Since the processing of data grounded on this purpose conveys high risks due to the amount of data processed, the GDPR requires the Members States to implement appropriate safeguards for data subjects’ fundamental rights and interest. As analyzed in Chapter 1 the disclosure of health data related in a work context may lead to the data subject facing stigmatization or discrimination.

**Substantial public interest.**91 When defining what “substantial public interest” means, the Member States should ensure that the processing is proportionate to the aim pursued and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.92

**For other specific reasons.**93 Foundations, associations or any other not-for-profit body with a political, philosophical, religious or trade union aim may process data related solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes. In this case the body has to implement the appropriate safeguards and the data cannot be disclosed outside that body without the consent of the data subjects.94 Health data can also be processed in case of any legal claim.95

**Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.**96 Researchers can use health data without asking for explicit consent if they respect Union and Member States’ law regarding having other safeguards in place in order to respect data subjects’ right to data protection. In

---

90 Article 9.2 b) GDPR.
91 Article 9.2 g) GDPR.
92 The Data Protection Report has proposed that data that is processed by public agencies are comprehended in the exception if the data has been sent in plain text within the frame of a case or the data is necessary to the processing of the case. SOU 2017:39 p. 42. This proposition has been criticized by the DPA for being conflicting with the requirement of substantial public interest. Datainspektionen, Remittering av betänkandet SOU 2017:39 Ny dataskyddslag, p. 12.
93 The Data Protection Report has proposed that public agency and organs that are comprehended by the principle of publicity can process data that has been sent to the agency and are required by law. In exceptional cases public agencies may also process data if it is absolutely necessary for the purpose of processing and the processing does not imply a breach of the data subjects privacy. SOU 2017:39 p. 172 f.
94 Article 9.2 d) GDPR.
95 Article 9.2 f) GDPR.
96 Article 9.2 j) GDPR.
this case, pseudonymisation\footnote{Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Article 4.5 GDPR.} is considered as one of the possible safeguards. If possible data should be anonymized. The Swedish Data Committee concluded that sensitive data should only be processed for statistical purposes if the social interest of the statistical project overweighs the risk for breach of the individuals’ privacy that the project might imply.\footnote{SOU 2017:39 p. 236.} The Committee has considered that this would be a safeguard as provided by the GDPR.\footnote{SOU 2017:39 p. 238. The DPA has criticized Data Protection Report regarding statement that the fact of the existence of implies that the law maker has assessed that the public interest overweighs individuals’ integrity. Datainspektionen, \textit{Remittering av betänkandet SOU 2017:66 Dataskydd inom Socialdepartementets verksamhetsområde}, p. 4 ff.}

Processing of health data under the form of registries that are used as base for scientific research is also bound to this regulation. Therefore, the registries must follow the safeguards established by the Member States according to article 89.\footnote{Recital 157 GDPR.}

5.1.3. Application of the Principle of least privilege in the GDPR

5.1.3.1. Purpose limitation

Purpose limitation is the first requirement that protects health data from being accessed by unauthorized users. In principle, Purpose limitation implies that ‘\textit{data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes}’.\footnote{Article 5.1 b) GDPR.} The purpose of the data processing will define the quantity, the type of data and the time during which the data may be processed. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization).\footnote{Article 5.1 c) GDPR.} Therefore, health care providers should limit the data they process only to the data necessary for the purpose of providing health care services that the patient is requiring. Furthermore, personal data may only be stored if they serve the purpose for which the data is processed (storage limitation).\footnote{Article 5.1 e) GDPR.}

Purpose limitation might imply indirectly that the data may only be processed by users that fulfill the purpose of the data processing established by the controller. For example, if the purpose of the processing is providing primary care services only the medical staff who

\begin{thebibliography}{99}
\item Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Article 4.5 GDPR.
\item SOU 2017:39 p. 236.
\item SOU 2017:39 p. 238. The DPA has criticized Data Protection Report regarding statement that the fact of the existence of implies that the law maker has assessed that the public interest overweighs individuals’ integrity. Datainspektionen, \textit{Remittering av betänkandet SOU 2017:66 Dataskydd inom Socialdepartementets verksamhetsområde}, p. 4 ff.
\item Recital 157 GDPR.
\item Article 5.1 b) GDPR.
\item Article 5.1 c) GDPR.
\item Article 5.1 e) GDPR.
\end{thebibliography}
provide medical attention may process the data provided by the patient. It is the controller who defines the purpose and who must provide instructions regarding how to process data according to this purpose.\footnote{\text{Article 32.4 GDPR.}}

Both the purpose limitation and the storage limitation have similar exceptions to its application. Further processing that is incompatible with the initial purposes of the processing is not considered incompatible if the data is processed to achieve purposes of public interest, scientific or historical research purposes or statistical purposes if the processing is subjected to appropriate safeguards.\footnote{\text{Article 89 GDPR.}} A similar exception is applied to the storage limitation. Personal data might be stored for longer periods than necessary for the purposes for which personal data is processed. Note that the principle of data minimization is not subject to the same exception. Consequently, regardless of the purpose for which health data is processed, the controller may not collect more data than necessary to provide the service offered to the data subject.

5.1.4. Appropriate Safeguards

As analyzed above, the processing of health data according to some of the exceptions in article 9.2. requires that the Member State implements appropriate safeguards in accordance to article 89. The Data Protection directive had the same requirement on article 8.4. The latter provision exemplified appropriate safeguard with limitation on search, access restrictions, access rights’ management and log audits and restrictions for which information that should be more available in an organization.

The Data Protection Investigation Commission considered that the above-named measures, in addition to requirement regarding pseudonymizing, direct access, encryption and requirement of consent are considered appropriate safeguards.\footnote{\text{SOU 2017:66 p. 285 ff.}}

5.1.5. Organizational and technical measures.

This requirement was already incorporated in the Data Protection Directive\footnote{\text{Article 17 Data Protection Directive.}} and is now incorporated in the GDPR. Article 32.1 GDPR states that ‘Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as
well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.’

Access control is both an organizational and technical measure. Who has access to what information is an organizational measure determined by the controller. At the same time, assigning reading rights to a user is a technical measure performed by the system operator.108

The provision was implemented in section 31 Data Protection Act. Although the disposition did not explicitly require the controller to limit the privileges assigned to a user to what he or she needs to complete a task, the Data Protection Authority already incorporated this principle as a part of its general advice and part of its established practice.109 The measure is also justified taking into account the severity for the rights and freedoms for natural persons of processing health data.110

To avoid unauthorized access and processing of data, the DPA requires the controller to use systems that allow auditing data access. Such a system should incorporate the possibility of identifying the user account and the natural person connected to that account. Moreover, the system only grants access those who need the specific personal data to execute their tasks. Furthermore, the controller must implement routines for managing privileges or rights of access and ensuring compliance.111 The question of establishing the limits of whom may have access to what are not discussed yet in regard to this regulation.

The GDPR imposes similar requirements. The GDPR specifies that the risks that should be considered are the likelihood and the severity for the rights and freedoms of natural persons. Furthermore, the GDPR states that the controller must follow-up and improve technical and organizational measures when necessary. The controller can demonstrate the compliance of this disposition by adhering to approved codes of conduct112 or using approved certification mechanisms.113

110 See Chapter 1.
111 Datainspektionen, Säkerhet för personuppgifter, Datainspektionens allmänna råd, p. 21. See also Datainspektionen 2003-2015 (2017-03-06).
112 Article 40 GDPR.
113 Article 42 GDPR.
In conclusion, both the data protection directive and the GDPR contemplate the implementation of organizational and technical measures to protect personal data from unauthorized access. In both cases the regulation includes access control, not because the regulation has specific requirements but because this is how the regulation has been interpreted according to best practice dictated by public authorities. In this regard, Member States have the possibility to establish in their national regulation further rules specifying organizational and technical measures.\footnote{Article 6.2 and 6.3 GDPR.}

5.1.6. Privacy by Design

Privacy by design is a concept that has been part of the standard requirements to comply with the organizational and technical measures that must be adopted by a controller. Privacy by design implies that data protection must be included from the onset of the designing of the system rather than including it at a later stage.\footnote{Article 25.1. GDPR.} This means that it is not enough to design a system and subsequently establish routines and policies establishing who can access what information. Access rights must be incorporated in the system, making it impossible or harder\footnote{Making access more difficult would be if e.g. if the user receives a warning that he or she is accessing information that they usually do not have rights to access.} for users to access data unlawfully or against the security policy.

Privacy by design implies mainly that mechanisms to protect integrity should be considered when developing the system in order to ensure e.g. that the amount of data that is processed is minimized to the amount strictly necessary for the purpose it is being processed, that the system is user friendly and at least transparent to the data subjects, that the access to data is limited and that the data is protected from unauthorized access.

The DPA states that limiting access to personal data is a crucial aspect of privacy by design. According to the DPA, the system must be able to manage rights of access in a way that adapts to the controller’s organization. Therefore, the controller should firstly review its working methods and ensure that they are able to assign access rights according to the security policy and regulation. An ideal system for access control should allow the user to access the right data easily while preventing the user from accessing data he or she does not need to fulfill his or her task. Data may be segmented based on e.g. membership in different groups or roles. The user should be able to have different roles in a system without being able...
to combine the access rights that are associated to the different roles at the same time.\textsuperscript{117} For example, a person may have an administrative role in a primary health care facility and at the same time have a nurse role. He or she will have the access rights corresponding to the role “administrative staff” and therefore access data needed to book medical attention. As a nurse, on the other hand, he or she might have access to a patient’s medical record. Nevertheless, when he or she is acting in the role of a nurse, she will not able to access data about patients’ appointments with other medical staff in the same facility. And when he or she is acting in the role of administrative personnel, he or she will not have access to patients’ medical records.

Another way to control access is by requiring documented reasons to access data that the user does not usually need to fulfill his or her tasks. The management of access rights should also be determined by the work flow limiting the access to registries and search possibilities. Furthermore, the DPA suggests encrypting stored data and providing the keys only to authorized staff.\textsuperscript{118}

5.1.7. Privacy by default

Privacy by default implies that the system’s workflow automatically directs the user towards an integrity-safe way of working and that the default settings are set in a way that not more than the necessary information is collected or shown to the user. In other words, the controller should ensure that only data strictly necessary for each specific purpose of the processing are processed by default. This has an impact on the amount of data processed, the extent of their processing, the period of their storage and accessibility.\textsuperscript{119}

Consequently, the data controller should limit the access to fulfill the purpose of data processing. Since every act of processing must be based on a legitimate purpose, privacy by default implies that only the users that process the data to achieve this purpose should have access to this data. In other words, this is another method of implementing the principle of least privilege in the GDPR.

\textsuperscript{117} Datainspektionen, Säkerhet för personuppgifter, Datainspektionens allmänna råd, p.21 ff.
\textsuperscript{118} Datainspektionen, Inbyggd integritet.
\textsuperscript{119} Article 25.2 GDPR.
5.1.8. Data Protection Impact Assessment (DPIA)

According to article 35 GDPR ‘where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. In this case the controller should seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment’.

The article 29 working group states that the processing of health data on a large scale is considered likely to result in a high risk, and requires a DPIA.\textsuperscript{120} The DPIA should comprise, inter alia, the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.\textsuperscript{121}

It is expected that one of the mechanisms of protection of personal data that the controller must report is the implementation of a policy for management of rights of access and compliance. Note that these requirements should be met before the processing of data.

5.2. Access control and application of the Principle of Least Privilege in the PDA

Unlike the GDPR the PDA contains specific regulation concerning management of access rights and supervisory access control. As mentioned in Chapter 2 access control is implemented through policies that determine who has access to what data. In the case of health care providers, access rights are regulated in the PDA. Note that this law is under revision due to the entry into force of the GDPR.

5.2.1. Scope of the PDA

Patient data is not defined, but for the purpose of this thesis, patient data is the data that is comprised by the scope of the PDA. Application of the PDA is limited to processing of

\textsuperscript{120} Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 Adopted on 4 April 2017, p. 8 f.

\textsuperscript{121} Article 35.7 d) GDPR.
personal data by health care providers in health care. The PDL applies to both manual and
digital processing of data that is related to both living and dead persons.\textsuperscript{122}

Health care providers are according to the PDL responsible for protection of personal data.\textsuperscript{123} 
This comprises even personal data processed by others on behalf of health care providers.
Health care providers are also responsible for the data processed by other health providers and
accessed directly according to the regulation regarding collaborative medical records.

Every person who processes personal data provided in this context is subject to this
regulation, regardless of their function.\textsuperscript{124} Therefore, the law is not only applicable to medical
staff but also managers of IT-systems are in the scope of this law. The law is also applicable to
employees who work on the IT department of a health care facility, as well as employees of a
company that provides cloud services to a health care provider.\textsuperscript{125} The health care provider
must ensure that all contractors or others that work for the health care provider or has contact
with the health care provider commit to protect patients’ data against unauthorized access.\textsuperscript{126}
The DPA has established that the PDA is applicable to contractors that provide medical aids
to patients as the requirement of managing these aids are directed to the health care
providers.\textsuperscript{127}

There are vast amounts of data that are collected by actors that do not provide health care
services. An example of this are health apps that can track an individual’s heart rhythm,
physical activity, hours of sleep, menstrual cycle among other health data. Health data can
also be obtained through patterns of search on search engines. Since this information is not
provided to health care providers it is not protected by the PDL. The GDPR may apply to this
type of data.

\begin{enumerate}
\item \textsuperscript{122} Chapter 1 section 1 PDA.
\item \textsuperscript{123} Chapter 2 section 3 PDA.
\item \textsuperscript{124} Prop. 2007/08:126 s. 238.
\item \textsuperscript{125} Fröberg, 2008, p.21 f. The contactor is a processor according to the GDPR, ie. a natural or legal person,
public authority, agency or other body which processes personal data on behalf of the controller. 4.8 GDPR.
\item \textsuperscript{126} Chapter 6 section 2 HSLF-FS 2016:40. When contracting services, the public health care provider should
ensure that the processor is also and persons who process data on his behalf are comprehended by professional
secrecy Chapter 25 section 1 Offentlighets- och sekretesslagen (2009:400). Persons who are not bounded by
professional secrecy cannot process data that requires professional secrecy even if they are bound by contractual
secrecy. JO 3032-2013 (2014-09-09). The DPA has required the government to incorporate legal secrecy
\item \textsuperscript{127} 3 b § Hälso- och sjukvårdslagen (2017:30).
\end{enumerate}
5.2.2. Which data may be processed?

The data that may be processed according to the PDA is the data that can be processed for the following purposes:\footnote{128}{Chapter 2 section 4 PDA.}

1) To fulfill the obligations of documenting information in a medical record and documenting other information that is necessary for the provision of health care to the patient.\footnote{129}{See 5.2.3.2. for more information about care-relationship.} This information includes, among others, the patient’s identity, relevant medical history, diagnoses and causes of treatments, information provided to the patient, relatives and treatment choices.

2) Administration regarding patients that are aimed to provide health care or are a direct cause of providing health care.

3) Document other data in accordance with law, regulations or other provisions.

4) Systematically and continuously develop and ensure the quality of the operations.

5) Administration, planning, follow-up, assessment and supervision of the operations or

6) Statistics regarding health care

The main carrier of patient’s data has previously been the medical record. Nevertheless, nowadays it is more accurate to refer to collections of personal data that are presented in different forms for the various actors in the health care sector. Health care IT-systems comprehend a huge number of systems and services that store and distribute data concerning patients.\footnote{130}{SOU 2016:41, p. 250.}

5.2.3. Who may access what?

The first question that is analyzed is who may access which data concerning patients. The answer will depend on whether the recipient works in the health care facility or process where the data has been collected or the recipient works for another health care facility or process.

Health care processes are defined as processes regarding health care that manage one or several related health problems or health status.\footnote{131}{2 kap. 1 § HSLF-FS 2016:40.} The delimitation of a health care process is functional and not organizational. A health care process may comprehend delimited activities in different health care units that have a functional connection. Health care units are defined
as organizational units that provide health care services. Examples of the latter are cancer units, emergency rooms and primary health care facilities. Hospitals are usually not one unit. The delimitation of a health care process and unit are determined by the health care provider.

5.2.3.1. Access to patient’s data within the same health care facility or process.

Inner secrecy applies within the same health care facility and between different health care units and processes. In general terms, Inner secrecy means that the receiver is not allowed to disclose information that is protected by professional secrecy. Nevertheless, the PDL’s interpretation of inner secrecy is broader than this. The main question is how to manage sensitive personal data concerning health or other personal data in order to decrease the risks of unauthorized access to data that may affect the patient’s integrity.

Chapter 4 Section 1 PDA stipulates that a person employed by a health care provider may access records concerning a patient if the person participates in the care of the patient or for other reasons needs information to fulfil a health care-related task.

A care relationship exists, e.g., between a treating physician and his or her patient when the patient is in the physician’s office. A care relationship often ends when the treatment of the patient ends, or the patient has not booked any further appointments with the physician. The latter is also applicable when the patient of a mental health unit is placed into the care of another health care provider. However, it is not always simple to determine whether a care relationship exists or not. This is the case of a family physician, who may provide care continuously to a group of patients. The care relationship will be maintained only if the physician and the patient have regular and frequent contact.

This provision is a clear application of the principle of least privilege in the access to health care data. It is only medical staff that may have access to patient data and only if they are directly providing a health care service to the patient in question.

---

132 Socialstyrelsen, Termbank.
136 prop. 2007/08:126 s. 252.
5.2.3.1.1. Active choice

When assigning access rights to employees, the health care provider must ensure that the medical staff cannot see that other care units or care processes store data concerning the patient.\textsuperscript{137} The medical staff will not have access to other data regarding the patient processed by the same health care unit or process unless he or she does not actively choose to access the patient’s data (active choice). An active choice means that an authorized user takes a stand regarding if he or she has right to access further data. An active choice implies that the user has assessed that he or she is authorized to access the data according to Chapter 4 PDA. Even after the employee has made the active choice data should not be available unless the staff make an active choice again. This active choice is meant to operate as a barrier to access the patient’s data.

With a first choice the employee will be able to see that there is data concerning the patient in another health care unit or process. If the employee decides that the data processed by other health care processes or facilities is necessary to provide care to the patient, the medical staff will have to make a second active choice to access this data.

5.2.3.2. Access to patient data processed by another health care unit or process

One of the novelties introduced by the amendment to the PDA was the possibility for authorized medical staff to direct access to information processed by another health care provider in the country, private or public. To accomplish this goal, the collaborative medical record was introduced in Sweden. All patients’ data do not have to be a part of the collaborative medical record, it can be limited to the parts that are documented in the medical record or other data regarding a patient.\textsuperscript{138} This implies that the health care providers may build up databases where only a specific type of medical data is available. The National Overview System\textsuperscript{139} is one of the examples of a system made to exchange data regarding a patient. The objective of regulation is to make it simpler and faster for health care staff to gain a complete picture of the patient’s health history no matter where in Sweden the patient has received health care previously. The general rule is that secrecy is applied to data within the public health care that are made available through collaborative medical records.\textsuperscript{140}

\textsuperscript{137} Chapter 4 section 4 HSLF-PS 2016:40.
\textsuperscript{138} prop. 2007/08:126 s. 248.
\textsuperscript{139} Nationell patientöversikt (NPÖ).
\textsuperscript{140} 25 kap. 1 § Offentlighets- och sekretesslagen (2009:400).
The term direct access used to describe the system implies the digital provision of data where the person responsible for the data does (controller) not have control over which that the receiver accesses at a specific time (automatized access) and where the receiver cannot alter the data in the system or register. Therefore, the receiver may access the data and read it, but not modify it.141

Medical staff may have access to patient data processed by another health care unit or process if the purpose of the processing is necessary to 1) fulfill the obligations of documenting information in a medical record and documenting other information that is necessary for the provision of health care to the patient. or 2) administration measures regarding the patient and that aims to provide health care in a particular situation or that are preceded by the provision of health care. Finally, the patient has consent to the processing of his or her data in the collaborative medical record.142 This is not a regulation regarding inner secrecy but concerning to the requirements for direct access to data processed by another health care provider. In practice, this means that the access to data is limited to the patients that have a care relationship with the health care provider.

If the system processes data that has not been blocked by the patient, the ‘new’ health care unit or process is able to see that there is information concerning the patient that is processed by another health care unit or process. Nevertheless, the medical staff from the new health care unit or process cannot access the data automatically. To access the data, the medical staff must have a care relationship to the patient in question; the data are presumed to have importance to prevent, assess or treat the patient’s diseases or injuries within the health care sector and the patient consents to access of his or her data.143 The consent must be informed, i.e., the healthcare provider must inform the patient that the consequences of collaborative medical records and that he or she has the right to block the access to these records. The direct access to the data is not possible if it does not comply with the requirements regarding collaborative medical records. For example, access to all the patient’s data in a municipality or county without the medical staff is not in accordance to the PDA. In the latter case a secrecy assessment should be made before disclosing a patient’s data.144

---

141 Prop. 2007/08:126 p. 105-106.
142 Chapter 6 section 2 § 5, PDA. This consent should comply with the requirements of article 7 GDPR in relation to Chapter 2 section 1 PDA.
143 Chapter 6 section 3 PDA.
144 Datainspektionen, 1567-2016 (2016-12-19).
The data might be accessed in cases of emergency without the patient’s consent. But the consent cannot be presumed only because the patient cannot give, or the patient is not able to understand the implications of consenting to processing of his or her information.

5.2.3.3. Direct access by third parties

Disclosure of personal data is only permitted if grounded in a legal provision. These legal provisions may be found, e.g., in some register laws. If a county or a municipality provide health care services through several public authorities, this county or municipality may have direct access to personal data processed by another authority within the same county or municipality.

5.2.3.4. Patients’ rights in relation to processing of personal data

The PDA allows health data to be processed without the patient’s consent. Even though there are requirements on informing the data subject about the processing, the data subject cannot oppose the processing. However, the patient can influence who can access the data and access data him or herself.

5.2.3.4.1. Patient’s consent

According to Chapter 4 PDA, medical staff within the same health care unit or process that processes information regarding a patient does not require the patient’s consent to access this data. The active choice is made by the medical staff. Regarding collaborative medical records, the patient does not have to consent for the information to be available to other health care units or processes. There is the obligation to inform the patient and the patient can oppose the processing of data, but the consent is not required. However, to access patient’s data, the member of staff that has a care-relationship to the patient needs the patient’s consent. The patient must be informed of the data being available to other health care providers. The health

---

145 ‘Third parties’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. 4.10 GDPR.
146 Chapter 6 section 4 PDA.
147 Chapter 2 section 2 PDA.
148 In this sense ‘consent’ should be interpreted in accordance to article 4.11 and article 7 GDPR. According to article 4.11 consent must be feely given. According to Article 29 Working Party has states that consent may only in exceptional cases be a valid ground for States to process personal data. Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, p. 15 ff. Therefore, processing of health data in collaborative medical record solely based on consent is debatable. SOU 2017:66 p. 226 ff. Consent regarding patients who are no able to consent in the long-term is being studied by the Government and an amendment to the PDA has been proposed. See Prop. 2013/14 p. 202.
care provider should decide on how to inform the patient regarding the circumstances. It is the health care provider that must prove that the patient has been informed. 149

A health care unit or processes may access data concerning the patient stored by other healthcare unit or process without the patient’s consent if the patient is temporarily unable to consent. If the medical staff assess that the data may be necessary for health care that the patient unavoidably needs the medical staff may access the data. 150

5.2.3.4.2. Patients’ right to block data

The DPA contains the right for the patient to block patient data if he or she does not wish other care units or care processes having access to his or her patient data. However, it will be visible for other care units and care processed that there is information that has been blocked.

Furthermore, the patient has the right to block other health care units or processes from accessing his or her data processed in collaborative medical records. The medical staff from the new health care unit or process will be able to see that the information is blocked, but will not be able to identify the health care provider who stores the blocked data. A patient that has chosen to block access to data may require the health care provider who has blocked it to unblock it.

In summary, the system is built so that medical staff has access to the information regarding the existence of patient’s data in another health care unit or process but not which. The second step is assessing if the existing information may be relevant to the patient’s health care and making an active choice to see where this data is stored. Knowing in which unit or process the information has been generated, the medical staff can assess whether the information is relevant for the patient’s treatment or not. Only information that may be relevant to the patient’s health care may be unblocked. The fact that the staff know that there is patient’s data in another unit or process might initiate a dialog between the patient and the staff in a situation. 151

Nevertheless, there might be situations when having access to the right information in time will be a matter of life and death. Therefore, the lawmaker has included an exception regarding blocked data. Medical staff may unblock data processed by the same health care

150 Chapter 6 section 4 § 2 PDA.
151 Prop. 2007/08:126 s. 249.
unit or process if the patient is not able to consent and it can have an impact on the patient’s care if it is necessary for health care that the patient unavoidable requires\textsuperscript{152} Medical staff is also authorized to unblock data if the patient’s life is in severe danger or in the case of a serious health hazard. The health care provider may even require the health provider who has blocked the data to unblock it if the data can be presumed relevant to the health care that the patient needs urgently.\textsuperscript{153} The patient in these cases can be, e.g., unconscious or too exhausted to decide.

If a patient, in one of those situations denies the unblocking of data this decision should be respected, regardless on if the patient seems to lack grounds or is irrational.\textsuperscript{154} But if access to the patient’s data is unavoidable due to the patient’s need of care the data might be accessed.

The implementation of patients’ right to block data has been under the DPA’s scrutiny. In June 2012 the DPA informed of the result of the supervision of 27 health care providers and stated that none of them complied with the regulation regarding blocking of data.\textsuperscript{155} A year later, after another inspection, the DPA could state that some health providers had made progress and were almost fully compliant. Other health providers, were still not complying with the regulation in the least.\textsuperscript{156}

5.2.3.5. Patients’ right to access data

The patient has the right to access his or her data according to the DPA. The data to which the patient may have access is the data contained in medical records and other documented data necessary for the patient’s health care and data used for an administration that aims to provide health care in specific cases or are preceded by health care.\textsuperscript{157} The patient may also access data that has been processed beyond the purposes established by the PDA with his or her consent.\textsuperscript{158} The patient may just directly access his or her data through strong authentication.\textsuperscript{159}

\textsuperscript{152} Chapter 4 section 5.
\textsuperscript{153} Chapter 6 section 4 PDA, prop. 2007/08:126 s. 243.
\textsuperscript{154} Prop. 2007/08:126 s. 243.
\textsuperscript{155} Datainspektionen, Datainspektionens nationella projekt om spärrar i IT-system inom hälso- och sjukvården.
\textsuperscript{156} Datainspektionen, Sammanfattning av Datainspektionens nationella projekt om spärrar i IT-system inom hälso- och sjukvården.
\textsuperscript{157} Chapter 6 section 5, PDA.
\textsuperscript{158} Chapter 6 section 5, PDA.
\textsuperscript{159} Chapter 4, section 11, (HSLF-FS 2016:40). Strong authentication means the verification of an identity by two ways (for example, password and mobile phone). A similar definition is found in definition in article 4.30 Directive on payment services in the internal where ‘strong customer authentication’ means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession
The health care provider may limit the data available through direct access. The reason for the limited direct access might be, for example, secrecy. Other information might be more adequate to disclose in person, for example, certain diagnoses and test results. In this case the health care provider should inform the limitation of access to the patient.

5.2.4. Implementation of access control in the PDA

5.2.4.1. Management of access rights

As previously mentioned, the general rule in the DPA is that users only should have access to the information they need to fulfill their tasks. It is also the health care providers responsibility to inform the staff about their access rights and access policies. Furthermore, the regulation requires that the health care provider assign access rights (or privileges) individually to each user. This is what according to the GDPR are considered as organizational measures.

This implies that no group accounts should be created. The lawmaker has remarked that too generous access rights may lead to unlawful spreading of personal data. The bigger an information system is, the more levels of access rights must be created. If the system does not allow the health care provider to limit the access to patients’ data, it constitutes unauthorized disclosure of patients’ data.

Regarding medical staff they must access the data needed to provide a good quality and safe health care. Staff who works with follow-up of activities, statistics, financial administration and similar activities that are not oriented to individuals should only have access to data that is indirectly related to patients. Access to code keys, ID-numbers, and other data directly related to specific patients should be the exception.

This also means that medical staff should not search for data regarding themselves. If a person wants access to patient data regarding him or herself, he must request it to the health care

(something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

160 Socialstyrelsen, Handbok vid tillämpningen HSLF-FS 2016:40, p. 54.
162 Socialstyrelsen, Handbok vid tillämpningen HSLF-FS 2016:40, p. 34.
165 Prop. 2007/08:126 s. 149.
provider through regular means.\textsuperscript{166} Reading patient’s records for educational purposes has also been qualified as a breach of data secrecy.\textsuperscript{167} Even if it is the patient that asked the medical staff to access their own data it is not allowed if there is no actual patient-health care provider relationship.\textsuperscript{168}

The access must have a relation to a task that is assigned by the controller. An example of this is the case of a member of administrative staff who was also absolved of charges of data breach. The member of staff has accessed a patient’s medical appointment information data to avoid seeing her. The personnel had a personal feud with the patient and wanted to avoid contact. Her employer stated that the staff was instructed in certain cases to avoid contact with patients. The Court interpreted that a part of her tasks was to avoid patients they had conflicts with.\textsuperscript{169}

This management of access rights should be based on a needs and risk analysis.\textsuperscript{170} Additionally, the health care provider should implement routines to change, delete and continuously follow-up the assigned access rights to ensure that these are accurate and updated.\textsuperscript{171} This management of access rights applies to access to patient data that is processed by another unit or processed by the same health care provider,\textsuperscript{172} as well as to access to patient data processed by another health care provider.\textsuperscript{173}

5.2.4.1.1. Needs and risk analysis

The health care provider has, according to the PDA, an obligation to perform a need and risk analysis when managing access rights in a system that processes patient data. According to the DPA, it is not enough to have a policy document, and it is not sufficient that the health provider assigns access rights based on professional profiles. For example, it is not compliant with the regulation to assign all the nurses the same access rights. The access rights should be individually determined based on the need for data that the specific person has and the risk that the access might convey.\textsuperscript{174} This analysis should be performed in relation to all the staff who has access to patient data, including those who work with statistics, economic

\textsuperscript{166} NJA 2014 s. 221 and Örebro Tingsrätt, 2014-12-17, nr B 3691-14.
\textsuperscript{167} RH 2002:36. See also Sundsvalls Tingsrätt dom 2015-04-01 nr 747-14.
\textsuperscript{168} Hovrätten över Skåne och Blekinge dom 2014-03-11 nr B 1532-13.
\textsuperscript{169} Hovrätten för Nedre Norrland dom 2012-11-29 nr B 606–12.
\textsuperscript{170} Chapter 4 section 2 HSLF-FS 2016:40.
\textsuperscript{171} Chapter 4 section 3 HSLF-FS 2016:40.
\textsuperscript{172} Chapter 4 section 2 PDA.
\textsuperscript{173} Chapter 6 section 7 PDA.
\textsuperscript{174} Datainspektionen, Hur förhindrar man obefogad spridning av patientuppgifter?
administration, IT and other tasks that are not directly related to health care provided to the patient.

When performing the analysis, the health care provider should identify and list all the tasks within the health provider’s operations, the different professional profiles as well as the tasks that each member of the medical staff has been assigned. Furthermore, the health care provider should identify, and list risks related to broad access rights. Finally, this analysis should be used to ensure that existing access rights correspond to the task that must be performed by the staff. These analyses need to be performed when implementing a medical record system and must be documented and informed to medical staff usually through work routines. The health care provider needs to prove to the DPA that these analyses have been made and how.175

According to the DPA’s recommendations, the health care provider should clarify and specify the content and scope of the different task. To achieve this, the health care provider must take the perspectives into account. The first one is the different categories of personnel based on the professional profile (e.g., nurse, midwife, surgeon), specific tasks assigned (e.g., booking appointments, heart surgeries, providing dialysis), operating methods and workplaces (e.g., surgical department, reception, emergency room, ambulance). The second perspective is to analyze the actual tasks that the employer will be executing. Therefore, it is not acceptable to assign general access rights to all the medical staff or according to only their professional license or role. The third perspective is determining which patient data does the different operations need to access the base of their operating methods, scope and the assigned tasks.176 Members of staff may also have different types of access rights depending on the circumstances. For example, a person can be a student doing an internship at a health care unit and be employed at the same health care unit at other times.177 The result of the need analysis usually leads to the creation of different profiles. The profiles in the directory may be harmonized with the access rights management system.178 There is commercial software that manages access rights and reviews changes in the access rights.

The DPA has, for example, established that the system does not comply with the PDA’s requirements if a contractor for medical aids (such as wheelchairs) has access to the data of

---

176 Prop. 2007/08:126 s. 149.
177 Prop. 2007/08:126 s. 149.
every patient that has access to these medical aids, whether the aid is provided by the contractor or not.\textsuperscript{179} It is also not sufficient that medical staff only have profiles considering the unit they work in, even if the unit is limited to a reduced number of patients.\textsuperscript{180}

When doing the risk analysis, the health care provider should assess if there is patient data or a group of patients that should be specially protected based, e.g., on treatment, diagnose, health care unit and or medical specialty. In order to implement data minimization, and therefore reduce the risk of data breaches, the health care provider should assess if the purpose of data directly related to a patient can be fulfilled with data that only indirectly is related to the patient.\textsuperscript{181} The risk analysis also needs to take into account what rights the user has, for example, if it is only reading rights or even editing rights.

The lawmaker has remarked that a patient’s right to block information does not mean a limitation on the obligation of the health care provider to do a risk analysis.\textsuperscript{182}

5.2.4.2. Compliance

The DPA does include not only a “preventive” access control but also a follow-up requirement. According to the DPA, the health care provider must ensure that patient data that are partly or wholly automatically processed are documented and can be controlled. Active choices should therefore be registered. The health care provider shall implement systematic and regular audits to detect if an unauthorized user has had access to patient data. This provision is applicable to both access within the same health care unit or process, and access to data processed by another health care unit or process.\textsuperscript{183}

The purpose of audits is to ensure that users do not use their access rights to read, modify or delete data that they are not authorized to process. An example is access to the medical record of a patient to whom the staff has no care relationship to.

In order to audit who has accessed what data and for which reason, the health care provider is responsible for providing documentation (logs) where it is clear 1) how the data has been processed (e.g. if it has been read, altered, disclosed or printed out), 2) in which unit or process the data has been processed, 3) the time of processing and 4) the user’s and patient’s

\textsuperscript{179} Datainspektionen 1863-2015 (2016-07-01).
\textsuperscript{180} Datainspektionen 581-2013 (2014-05-07).
\textsuperscript{181} Propositionen 2007/08:126 p. 149.
\textsuperscript{182} I propositionen 2007/08:126 p. 152.
\textsuperscript{183} Chapter 4 section 3 PDA.
identity. The health care provider is also responsible for 1) systematic and regular sample controls of the logs, 2) documenting the control of logs and 3) storing the logs for at least five years to allow the supervision of access to patient data. It is the health care providers’ responsibility to prove to the DPA that such logs exist.¹⁸⁴

The DPA recommends the health care provider to inform the staff that log audits are implemented. This should have a preventive effect.¹⁸⁵ Since the unlawful access to patient data is a crime,¹⁸⁶ the real possibility of being discovered might deter medical staff from the unauthorized accessing of patient data. Therefore, the staff should also be informed about the consequences of the unauthorized accessing of patient data. This implies that the health care provider must define in a routine what unauthorized access means. It is not enough to state that logs will be controlled if there is any suspicion of unauthorized access. Otherwise the log audits might be useless.¹⁸⁷ The staff that audits the logs must also have routines that establish in which cases they need to investigate further.¹⁸⁸

The log audit should according to the DPA follow specific parameters. An example of these parameters are: controlling the access to a specific patient’s data, access by a particular employee, when information regarding a patient has been accessed several times (more than usual), information that has been accessed at unusual times of the day, access to protected personal data, access to data regarding children, access to data concerning famous persons, data from specific health care facilities or medical specialties, and access to blocked data.¹⁸⁹

The health care provider must implement a routine for log audits that determine how often they will take place and how much data will be analyzed. The number of logs that must be controlled will depend on the size of the health care provider’s operations. The critical aspect is that the purpose of the log audits is reached, i.e., detecting unauthorized access to patient data and preventing future unauthorized access.¹⁹⁰ The DPA also recommends examining the

¹⁸⁴ Chapter 5 section 9 HSLF-FS 2016:40.
¹⁸⁶ According to Chapter 4 section 9c Penal Code “A person who unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for at most two years. The same is applicable to a person who, through a similar action seriously disturbs or prevent the use of such data”.
¹⁸⁹ Datainspektionen, Systematisk logguppföljning.
¹⁹⁰ Prop. 2007/08:126 s. 150.
possibility of implementing system solutions that could make the log audits simpler, such as automated log analysis tools.\textsuperscript{191}

The patient is also allowed to access the logs to know who has accessed his or her data.\textsuperscript{192} The purpose of this provision is to make the health care system transparent and allow the patient to know who has accessed his or her data and eventually calm any fear of breach of data secrecy. However, the lawmaker has concluded that there is no need to identify specifically members of the medical staff or to have access to other data that indirectly is related to a natural person.\textsuperscript{193} The information that the patient can access is the name of the unit of process that has accessed the information and on which date. If the health care provider is public, the log lists are public documents that may be disclosed according to Chapter 2 Freedom of the Press Act.\textsuperscript{194}

Auditing access might lead to certain privacy risks affecting the user. For example, if the purpose is to trace what employees have done in a case management system, it might lead to processing of sensitive data of a person related to the case. The Data Privacy Commission has declared that lawmakers should take this privacy risks into consideration and assess them in relation to the privacy benefits before introducing provisions regarding log controls.\textsuperscript{195} Log controls are part of a process of data with the aim of regularly testing, assessing and evaluating the effectiveness of technical and organizational measures. According to article 32.1 d) GDPR it may be appropriate to ensure an appropriate security level to these processes.

One of the greatest challenges of implementing log audits is the large number of it-systems used by different health providers. This creates difficulties for the systems to communicate and, therefore, to create logs whenever data is accessed.\textsuperscript{196}

5.3. Access control and application of principle of least privilege in register laws

In this part the analysis focuses on register laws that allow the processing of health data. The content of these register laws is varied and refer to different data. Without the existence of a

\textsuperscript{191}Datinspektionen, \textit{Systematisk logguppföljning}. See also Socialstyrelsen, Handbok vid tillämpningen HSLF-FS 2016:40, p. 52.
\textsuperscript{192} Chapter 8 section 4 PDA.
\textsuperscript{193} Chapter 4 section 10 HSLF-FS 2016:40.
\textsuperscript{194} Tryckfrihetsförordningen (1949:105). This is applicable even when the medical staff has not signed the medical record. HFD 2013 ref 33.
\textsuperscript{195} SOU 2017:66 p. 286 f.
\textsuperscript{196} SOU 2016:2, s. 285 ff.
law the controller is not allowed to process data in a registry. Furthermore, health data must be processed by or under the responsibility of a professional subject to the obligation of professional secrecy. Note that all the laws and regulations analyzed in this section are subject to review due to the entry into force of the GDPR.

The Official Report of the Swedish Government ‘Data protection in the Ministry of Health and Social Affairs area’ classifies the registry laws and regulations that are analyzed in this section into: 1) those that regulate a certain activity i.e., PDA and Pharmacy Data Law\textsuperscript{197} and 2) those that regulate a register or collections of information i.e. Act on Pharmacopeia,\textsuperscript{198} Health Data Register Act,\textsuperscript{199} Act on National Vaccination Program Register\textsuperscript{200} and the Medicinal Products Act.\textsuperscript{201} There are also other laws that contain provisions that regulate processing of personal data. The latter laws are not analyzed in this section. In addition, laws that regulate registries that process health data for research purposes, e.g. the Act on certain registers for research into the impact of genetics and environment on people’s health,\textsuperscript{202} are also analyzed.

5.3.1.1. Type of health data processed by registries

The information processed by the controllers of this registries is varied. It is usually the health care provider who has initially collected the information who is responsible for reporting it to the controller of the registers. The main purposes of the processing of health data in these register laws are administrative purposes,\textsuperscript{203} reporting to supervisory authorities, relation to the patient, statistical purposes and quality improvement of the health care provider, as well as research purposes. Only the last two purposes will be analyzed.

5.3.1.1.1. Statistics, follow-up and quality improvement of the operations

Some registries process data for statistical purposes. This is the case of the Health Data Register Act that allows the National Board of Health and Welfare to process personal data for statistical purposes. The scope of this register law is vast and therefore several regulations

\textsuperscript{197} Apoteksdatalag (2009:367).
\textsuperscript{198} Lag (2005:258) om läkemedelsförteckning. The Government has proposed that a new Act on Nation Phacopeia is enacted. This law would replace the current Act on Pharmacopeia and Prescription Register Act and should enter into force 1st July 2018. Ds 2016:44.
\textsuperscript{199} Lagen (1998:543) om hälsodataregister.
\textsuperscript{200} Lagen (2012:453) om register över nationella vaccinationsprogram.
\textsuperscript{201} Läkemedelslag (2015:315).
\textsuperscript{202} Lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.
\textsuperscript{203} See, for example, sections 8.4 and 8.5 Pharmacy Data Act.
specify which data may be processed and for what specific purpose. Among the registers that are grounded in this law are:

- **Patient register.**204 This register contains personal data from patients that have been placed in institutional care, have been treated by physicians other than primary health care or have been treated by medical staff other than physicians within the non-institutional psychiatry care. The data processed in this register is, inter alia, ID number, gender, birth year, diagnoses, measures, causes of the disease or injury.

- **Medical birth register.**205 This register processes data regarding the newborn (id number, the city of registration) and the mother and eventually the father. The register includes data such as the number of pregnancies of the mother, use of tobacco and pharmaceuticals before and during the pregnancy, occupation, citizenship of the newborn’s parents, total number of children, among others.

- **Cancer register.**206 This register contains data regarding patients who have been diagnosed with tumors or a similar diagnose. The personal data that may be processed is a name, ID number, diagnoses, expansion of the tumor, among others.

Furthermore, other register laws allow the processing of personal data regarding patients for other purposes than the ones mentioned above. Information regarding vaccination such as date of the vaccine and data to identify the person who received the vaccine may also be processed for statistical purposes.207

The PDA is also applicable to personal data that are processed in quality registries. Quality registries are an automatized and structured collection of personal data that has been created to systematically and continuously develop and ensure the quality of health care. Quality registries should allow comparisons in between health care on a national and regional level.208 Therefore, personal data processed in a quality record is collected by several health care providers. Unlike patient data, personal data in quality registries may not be processed if the patient opposes processing of her or his data. Furthermore, if the individual whom the data concerns opposes the processing, the personal data should be deleted without delay.209

---

204 Förordning (2001:707) om patientregister.
207 Section 6.1 and section 7 Lagen (2012:453) om register över nationella vaccinationsprogram.
208 Chapter 7 section 1 PDA.
209 Chapter 7 section 2 § 2 PDA.
According to Chapter 7 section 4, personal data in national quality registries may be processed to systematically and continuously develop and ensure the quality of the health care. Data processed for this purpose may also be processed to obtain statistics, health care research, and report data to a controller that will use personal data for these latter purposes and fulfillment of another legal obligation of providing data. Only personal data that are necessary for the purposes previously mentioned may be processed in a national or regional quality register. An individual’s identification number or name may be processed in a national or regional quality register only if coded personal data or personal data that only indirectly can be linked to the individual is not enough to fulfill the purposes previously mentioned. Sensitive personal data that are not related to health can only be processed if there is an explicit authorization by the government. A health care provider can have direct access to the information saved in a quality record. In the latter register, ID number may only be processed if the coded personal data is not enough to fulfill the purpose of the processing.

This type of purpose is also applicable to retail pharmacies.

5.3.1.1.2. Research

All the data processed according to the Health Data Register Act, Quality registers and Act on National Vaccination Program may be processed for research purposes and epidemiological studies. Furthermore, there is special legislation that regulates the ethical review of research involving humans. This legislation applies to research that involves humans or human biologic material, and that entails processing sensitive data. This type of research is therefore subject to an ethical assessment. The main rule is that research can only be approved if it can be done concerning the human value and that the welfare of humans is prioritized in relation to the needs of society and the scientific community. Furthermore, research cannot be approved if the same result can be reached by methods that imply lower risks to a person’s health, security and integrity. The person's integrity therefore limits the data processed by a research project. The general rules are that the data subjects need to give his or her consent for

210 Chapter 7 section 8 PDA.
211 Chapter 7 section 9 PDA.
212 Section 8.10 and 8.11 Apoteksdatalagen (2009:367).
213 Lag (2003:460) om etikprövning av forskning som avser människor.
214 Section 7 and 8 Lag (2003:460) om etikprövning av forskning som avser människor.
215 Section 10 Lag (2003:460) om etikprövning av forskning som avser människor.
the processing of the data to be legal.\textsuperscript{216} To process data in the research registries, we analyze the research must be approved by the Regional Ethical Review Board.

There is also one specific register law that regulates certain registers for research into the impact of genetics and environment on people’s health.\textsuperscript{217} This law regulates personal data processed by universities and institutions of higher education and states that personal data may only be processed to create the basis for a research project into the impact of genetics and environment on diseases and people’s health and to disclose this information legally.

The possibility of introducing a law that regulates protection of data subject to research has been proposed in the Official report of the Swedish Government ‘Processing of personal data for research purposes’.\textsuperscript{218}

5.3.1.2. Access control and implementation of the principle of least privilege

5.3.1.2.1. Access by the controller

Firstly, the controller may process the data processed in the register. Following the principle of least privilege, most of the register laws contain provisions that state that users only should have access to the information they strictly need to fulfill their tasks. Their tasks, in accordance with the purpose limitation, must be related to one of the legal purposes of data processing.

5.3.1.2.2. Direct access by third parties

According to the various register laws, there are several authorities and actors that may have access to the personal data contained in the different registries. In this part, we focus on what is called “direct access”, which means that natural persons, companies, organizations and other public authorities can search in a register and databases which usually are not available. The main characteristic of direct access is that it is immediate and that a secrecy examination is performed when implementing the direct access in the regulation and not every time a user accesses the data in the register. On the contrary, when there is no direct access but ‘normal’ disclosure of information the public authority must perform a secrecy examination every time it receives a request for data. In theory, the difference between direct access and disclosure

\textsuperscript{216} Section 12 Lag (2003:460) om etikprövning av forskning som avser människor.
\textsuperscript{217} Lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.
\textsuperscript{218} SOU 2017:50 s. 118.
might seem clear, but they might seem similar when, e.g. public authorities use automatized systems to disclose data.\textsuperscript{219}

Direct access to data pressuposes the existence of a provision that allows it explicitly. In the Act on Pharmacopeia, the prescriber of the medicine, licensed nurses without the lincense to prescribe medicines and pharmacists may have access to data in the register, if the data subject has given his or her consent for these persons to access the data.

The Health Data Register Act, on the other hand, only allows the controller, i.e. the National Board of Health and Welfare to directly access data in the health data register. Similarly, the PDA allows health care providers to access data they have registered in the Quality Registries.\textsuperscript{220}

5.3.1.2.3. Access by the data subject

Some of the register laws contain provisions that allow the data subject to access his or her data directly. This is the case of the Act of Prescription Register, which does not set any limitations to the data the data subject may access.\textsuperscript{221} The Act of Pharmacopeia has a similar provision in section 7.

5.3.1.3. Access control in register laws

Regarding processing of data in registries it is frequent that persons that do not work under the controller’s supervision, especially in the case of processing of data for research purposes. In consequence, access control regulation may apply to receivers that have an independent responsibility for protection of personal data. Nevertheless, access control is a security measure that decreases the risk of unauthorized access to health data and should, therefore, be implemented by the controller.\textsuperscript{222}

As mentioned above, processing of data in a register supposes the existence of a law that authorizes the processing of data. Therefore, a processor cannot process data from a register if the processing lacks legal grounds. This is the case of the research study ‘Stockholm Health’ that Statistics Sweden was to perform in behalf of Stockholm’s county. The research project’s objective was to determine the frequency of certain illnesses and how to prevent them. The

\begin{footnotesize}
\textsuperscript{219} HFD:s dom 2015-10-19 i mål nr 1356-14.
\textsuperscript{220} Chapter 7, section 9 PDA.
\textsuperscript{221} Section 11 Lag (1996:1156) om receptregister.
\textsuperscript{222} SOU 2017:50, p. 260.
\end{footnotesize}
project implied that Statistics Sweden would link the data it processed to health data that belonged to the county’s competence, as well as to the data processed by two other public authorities. The DPA concluded that Statistics Sweden had no legal grounds to process this sensitive data for this purpose and ordered it to cease the processing.\textsuperscript{223}

5.3.1.3.1. Management of access rights

Access control mechanisms are regulated in a similar way to the ones regulated on the PDA. For example, the Prescription Register Act states that the E-health authority (the controller according to section 5) should determine the conditions to assign rights of access to partially or wholly automatically processed patient data. The access rights shall be limited to what the employee at the E-health authority needs to fulfill his or her tasks.\textsuperscript{224} Similar provisions are found in the Act on Pharmacopoeia,\textsuperscript{225} Pharmacy Data Act,\textsuperscript{226} the Act on National Vaccination Program Register\textsuperscript{227} and the Act on certain registers for research into the impact of genetics and environment on people’s health.\textsuperscript{228} There is no similar provision in the Health Data Register Act. Nevertheless, the latter law’s government bill stated that the security measures regulated in section 31 of the Data Protection Act would be applicable, and that according to the DPA this entailed the implementation of access rights management and compliance.\textsuperscript{229}

According to the DPA it is the controller’s responsibility to ensure that data that is disclosed according to the registry laws are processed by authorized users. In 2010 the DPA’s supervision of quality registries showed that health care providers disclosed data to the quality registers without knowledge of who was receiving the data, using open networks to transfer patients’ data.\textsuperscript{230} The DPA also noted that the existence of economic incentives for each patient registered in a quality register affected the health care providers’ inclination to comply with data protection regulation.\textsuperscript{231}

\textsuperscript{223} Datainspektionen 290-2016 (2016-12-19).
\textsuperscript{224} Section 22, Lagen (1996:1156) om receptregister.
\textsuperscript{225} Section 12 a Lagen (2005:258) om läkemedelsförteckning.
\textsuperscript{226} Section 12, Apoteksdatalagen (2009:367).
\textsuperscript{227} Section 9, Lagen (2012:453) om register över nationella vaccinationsprogram.
\textsuperscript{228} Section 10, Lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.
\textsuperscript{229} Prop. 1997/98:108, p. 84 f.
\textsuperscript{231} Datainspektionen 1049-2012 (2913-03-15).
5.3.1.3.2. Compliance

The mechanisms to audit access to health data is also regulated in some of these laws. For example, the Pharmacy Data Act states that the pharmacy license holder should ensure that access to data that is wholly or partly processed automatically, regarding consumers and those who have a license to prescribe medicines, is documented so the access to this data can be audited. The same dispositions can be found in the Act of Pharmacopeia.

5.4. Conclusions and remarks.

Access Control regulation has been incorporated into the regulation concerning processing of health data, the form of management of access rights and compliance, i.e., log audits. Access control is both a technical and organizational security measure that is an essential part of information security. Therefore, healthcare providers must implement access control to comply with information security requirements on the GDPR and the PDA. The security policies that determine who can access which data are not only defined by the controller. The lawmaker, both European and National, has decided that access rights should only be assigned to users who need the data to fulfill a task. This is a manifestation of the principle of least privilege in the regulation of health data processing.

Previous data protection regulation focused on establishing obligations for the controller regarding the security of the system without specifying how these security measures should be implemented. The lawmaker has now gone one step further in the GDPR. It is now not enough that the controller implements organizational and technical measures to protect the data ex post, but these measures must be designed in the system that processes personal data. As a result, the controller must incorporate mechanisms of access control in the system. This requirement was previously part of the DPA’s practice, but was not a legal requirement.

The principle of least privilege has been incorporated into the GDPR, PDA and register laws. This principle plays not only a role for information security, but also to protect data subjects' privacy. This is central since the processing of health data is often permitted without the data subject's consent.

The controller’s responsibility specifies which task will be performed by whom and assign access rights that correspond the tasks assigned to an employee. Therefore, to comply with the

233 Section 12 b Lagen (2005:258) om läkemedelsförteckning.
principle of least privilege the controller needs to perform need and risk assessments when assigning access rights or privileges to its employees. The assignment of access rights also must be individual, considering the tasks to be performed by each employee. Applying this principle implies creating both technical and organizational conditions for compliance.

Determining if data is necessary to fulfill a task may not be the simplest undertaking. Several resolutions from the DPA show that there are still organizational and technical issues that hinders compliance of access control regulation and the principle of least privilege. Organizational barriers might consist e.g. on the controller not defining what unauthorized access is, assigning broad access rights and assigning access rights in relation to roles instead of tasks. The technical barriers consist mainly on different healthcare providers having different systems which makes e.g. log controls more difficult, systems not being able to block patient’s data or systems allowing users to access more data than they need to fulfil their tasks.

When applying the principle of privilege, the healthcare provider must consider the patients’ rights according to the Patient Act, i.e., the right to self-determination, to participate in his or her own health care and the respect of patients’ privacy. These pillars of the healthcare are reflected in the patient’s right consent to processing in collaborative medical records, active choice and the right to block data. These rights might at first seem incompatible with the principle of least privilege if the defined task is to provide good quality health care. Requirements of consent, active choice and the right to block data may affect the availability of the data and prevent the patient from getting the benefits of analyzing a large amount of data concerning his or her health to be able to provide a more accurate diagnosis. In this sense, the patient’s integrity and self-determining right seems to outweigh the need of information of the medical staff to make good medical decisions. The reason behind this might be that in the overall picture, the consequences of breaches on data privacy in the health care sector have severe consequences, as analyzed in Chapter 1.
6. Conclusion

The digitalization of health data is growing rapidly. It started with the digitalization of medical records and services to book medical appointments and has evolved to the provision of medical services. These digital medical services are directed both to medical staff and patients. Digital tools allow a more accurate and fast diagnosis and following treatment as well as providing the patient with information about his or her health. Data concerning health is also provided freely by individuals, not only to healthcare providers but also to private companies that offer devices and apps that allow users to track health information about themselves. Digital tools are not only used for curative health care but also for preventive health care.

The tendency shown is that health care, in the future, will focus on the patients’ self-care, allow more personalized diagnosis and treatments, and smart homes will provide health Care to individuals in the comfort of their homes.

The increasing of the digitalization of Health Data has led to the incorporation of a definition of 'data concerning health' in the GDPR. This definition is relevant because the data concerning health is classified there as sensitive data, which imposes certain legal requirements, such as professional secrecy, for the data to be processed.

The evolution of digitalization in the healthcare sector entails an increasing amount of health data being processed by a large number of controllers, so called ' big Health Data'. This phenomenon, as well as the fact that some important health Data, such as the one provided by DNA, remain relevant, increasing risk of breaches of data privacy.

Breaches of data privacy in the healthcare sector can have severe impacts both on the data subject, health care providers and Society. The unlawful disclosure of the most sensitive data, such as those related to mental health and sexual health, might lead to harm on the reputation, discrimination, mistrust on the healthcare provider and even result in risks for the patient's safety and life. The patients' mistrust in the healthcare system might lead to worsened public Health. Unlawful disclosure of healthcare data might also lead to loss of freedoms and individuality, depending on the purpose of the receiver.
The severe impact that breaches of health data privacy may entail highlights the importance of regulating requirements concerning information security. Health Data protection regulation requires controllers to ensure confidentiality, integrity and availability of health data. Access Control is one of the pillars of information security. Access control as a function controls that the user who requests access to a system resource, i.e. health data, is authorized to access the data. Access control also presupposes securing that the user is the natural person who is authorized to access the requested data and compliance through log audits. This function operates not in relation to a user’s request to a system but also other systems’, processes’ and programs’ requests of data. Therefore, this function is used to prevent unauthorized or unlawful access to data. Access control mainly focuses on the confidentiality of the data, but also protect the integrity and availability of it, as it prevents unauthorized users to unlawfully modify or delete data.

Who can access what is determined by an access policy that, according to best practice, should apply the principle of least privilege. According to this principle, users should only be able to access the data they need to fulfil a task. Thus, this principle reduces the vulnerability of a system. The impact of, e.g., social engineering attacks is limited to the resources the users have rights to access. At the same time, in the context of health care, the principle of privilege also has a role in protecting data subjects’ privacy.

Both access control and the principle of least privilege have been incorporated to laws and regulations concerning processing of health data. Regarding access control there is at times a terminological difference. Some laws, such as the PDA and the Pharmacy Data Act, regulate under the title ‘access control’ (åtkomstkontroll) the audit of logs. As mentioned above, log audits are a mechanism to ensure compliance with the access policy implemented by the controller. Thus, the concept of access control in the PDA and register laws that contain provisions concerning access control, focus on the compliance of the access policy, rather than the access to the data itself. Access control requirements on systems that process health data are imposed by the DPA and are based on best practice.

The principle of least privilege is explicitly contained in several provisions, in the PDA and register laws, that regulate management of access rights. These provisions follow the principle of least privilege by providing that users can only access data that is necessary to fulfil a task. In the health care sector, the general rule is that only medical staff that have a care-relationship to the patient may access the patient’s data.
The task that a user will perform is central to define his or her access rights. In general terms, this task is defined by the controller. This assignment of tasks is the base for a need analysis that responds to the question: does this user need access to this data in order to fulfill a task? Furthermore, the controller must analyze the risk of processing the data. This risk analysis must address the question on whether the user needs data that is directly related to the patient, if it is sufficient that the data is only indirectly related to the patient or if the data can be anonymized. For example, in the case of data processed for statistical or research purposes, the controller must consider pseudonymising data.

The DPA’s supervision has shown that many health care providers do not fully or only partially comply with the access control regulation. Incompliance with access control regulation usually consists on assigning broad access rights to roles in the organization, due to assigning access rights to roles in the organization and being unable to define what unauthorized access is. Furthermore, some health providers fail to comply with log audits, and some of them do not create logs of data processing.

The answer to the question of what data the user needs to be able to fulfil a task is not an easy one. The task is limited by the purpose of processing according to the GDPR. In the debate of how much information a controller should be allowed to access Official Reports of the Swedish Government show an increasing need from controllers who process health data to be able to access more data. In the case of health care providers, limiting their access to data may limit the possibility of using new technologies that would allow improving effectiveness and quality in health care. In the case of controllers that process health data for statistical and research purposes, the limitation of access to data prevents them from using ‘big health data’ to study illnesses and medical issues in the population and how to prevent them.

Two of the tendencies in health care, as mentioned above, are patients’ self-care and health care provided at home. This will be the result of an increasing automation in health care services. As a result, the user-to-system interaction will decrease, while the system/process/program-to-system interaction will increase. Requirements on security measures, such as access control, that are incorporated into systems by design or by default have just been incorporated by the GDPR. Automation may lead to the incorporation of requirements, especially on system-to-system access control, where the principle of least privilege should be applied by default in order to take advantage of new technologies in health care at the same time that the privacy of patient’s is protected.
7. Bibliography

7.1. Books


7.2. Journals and articles


7.3. **Electronic Sources and web pages**


Memorial Sloan Kettering Cancer Center, *Memorial Sloan Kettering Trains IBM Watson to Help Doctors Make Better Cancer Treatment Choices*, “https://www.mskcc.org/blog/msk-
trains-ibm-watson-help-doctors-make-better-treatment-choices”, last accessed on 2017-12-24 [cit. Memorial Sloan Kettering Cancer Center]


Socialdepartementet & Sveriges Kommuner och Landsting, Vision e-hälsa 2025 - gemensamma utgångspunkter för digitalisering i socialtjänst och hälso- och sjukvård, 2016-03-10, ”http://www.regeringen.se/contentassets/79df147f5b194554bf401dd88e89b791/vision-e-halsa-2025.pdf”, last accessed on 2017-12-23. [cit. Socialdepartementet & SKL, Vision e-hälsa 2025].


8. Table of Statutes, Conventions and Preparatory Works

12.1. European Union

12.1.1. Statues and conventions


12.1.2. Recommendations

Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data (Adopted by the Committee of Ministers on 1997-02-13 at the 584th Meeting of The Ministers' Deputies).

12.1.3. Preparatory work

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 Adopted on 4 April 2017, available at “ec.europa.eu/newsroom/document.cfm?doc_id=441372”, last accessed on 2017-10-06.

12.2. Sweden

12.2.1. Statutes

Tryckfrihetsförordningen (1949:105).
Offentlighets- och sekretesslagen (2009:400)
Brottsbalk (1962:700).
Lag (2003:460) om etikprövning av forskning som avser människor.
Lag (2005:258) om läkemedelsförteckning.
Lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.
Häls- och sjukvårdslagen (2017:30).
Inspektionen för vård och omsorgs föreskrifter (HSLF-FS 2017:41) om anmälan av händelser som har medfört eller hade kunnat medföra en allvarlig vårdskada.
Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

12.2.2. Preparatory Works

12.2.2.1. Government memorandums

Ds 2016:44 Nationell läkemedelslista.
12.2.2.2. Government bills

Prop. 2007/08:126 om patientdatalag m.m.
Prop. 2013/14:202 om förbättrad informationshantering avseende vissa patienter inom hälso- och sjukvården.

12.2.2.3. Swedish Government Official Reports

SOU 2006:82 Patientdatalag.
SOU 2014:23 Rätt information på rätt plats i rätt tid.
SOU 2014:45 Unik kunskap genom registerforskning.
SOU 2016:2 Effektiv vård.
SOU 2017:50 Personuppgiftsbehandling för forskningsändamål.

12.2.2.4. Submission for comment

13. Table of Cases

13.1. Civil, penal and administrative courts

NJA 2014 s 221.
HFD 2013 ref 33.
HFD:s dom 2015-10-19 i mål nr 1356-14.
RH 2002:36.
Kammarrätten i Stockholm dom 2015-12-02 nr 7632-15.
Hovrätten för Nedre Norrland dom 2012-11-29 nr B 606-12.
Förvaltningsrätten i Stockholm, 2016-10-28 nr 14576-16.
Örebro Tingsrätt, 2014-12-17, nr B 3691-14.

13.2. Parliamentary Ombudsmen

JO 3032-2013, dated 2014-09-09.

13.3. Data Protection Authority

Datainspektionen 1606-2009 (2010-10-11).
Datainspektionen 920-2012 (2013-08-26).
Datainspektionen 1568-2014 (2014-12-08).
Datainspektionen 1567-2016 (2016-12-19).
Datainspektionen 290-2016 (2016-12-19).
Datainspektionen 2003-2015 (2017-03-06).

13.4. Health and Social Services Inspectorate

Inspektionen för vård och omsorg, 33230/2015 (2016-06-30)