Decision

Diarienr

2020-12-02

DI-2019-3840

The board of Sahlgrenska

University Hospital

Blue stripe 5

413 45 Gothenburg

Supervision under the Data Protection Regulation and

Patient Data Act - needs and risk analysis and

questions about access in journal systems

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

Content

The Data Inspectorate's decision

During an inspection on 23 April 2019, the Data Inspectorate has established that

The board of Sahlgrenska University Hospital (Sahlgrenska

University Hospital) processes personal data in violation of Article 5 (1) (f) and

5.2 and Article 32 (1) and (2) of the Data Protection Regulation1 by:

1.

Sahlgrenska University Hospital as

personal data controller does not meet the requirement that it should have

carried out a needs and risk analysis before allocating

permissions are made in the journal systems Melior and Nationell

patient overview in accordance with ch. 4 § 2 and ch. 6 § 7

the Patient Data Act (2008: 355) and ch. 4 Section 2 of the National Board of Health and Welfare

regulations and general guidelines (HSLF-FS 2016: 40) on record keeping

and processing of personal data in health care. This

means that Sahlgrenska University Hospital has not taken

appropriate organizational measures to ensure and be able to

show that the processing of personal data has a security that is

appropriate in relation to the risks.

2. Sahlgrenska University Hospital does not restrict users

permissions for accessing the Melior and National journal systems

patient overview to what is only needed for the user to

be able to fulfill their duties in health care

according to ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and Chapter 4 2 § HSLFFS 2016: 40. This means that

Sahlgrenska University Hospital does not

has taken steps to be able to secure and be able to show one

appropriate security for personal data.

3. Sahlgrenska University Hospital does not have documentation in Melior

of access (logs) where it is stated which measures have been taken

with information about a patient according to ch. 4 Section 3 of the Patient Data Act and 4

Cape. § 9 (point 1) HSLF-FS 2016: 40. This means that Sahlgrenska

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection

for natural persons with regard to the processing of personal data and on the free flow

of such information and repealing Directive 95/46 / EC (General

Data Protection Regulation).

1

3 (34)

The Data Inspectorate

DI-2019-3840

The University Hospital has not taken appropriate organizational measures

measures to ensure and be able to demonstrate that the treatment of

the personal data has a security that is appropriate in relation to

the risks.

The Data Inspectorate decides on the basis of Articles 58 (2) and 83 of the Data Protection Ordinance and Chapter 6. § 2 of

the law (2018: 218) with

additional provisions to the EU Data Protection Regulation that

Sahlgrenska University Hospital, for violation of Article 5 (1) (f) and

5.2 and Article 32 (1) and (2) of the Data Protection Regulation, shall pay a

administrative penalty fee of 3,500,000 (three million five hundred

thousand crowns.

The Data Inspectorate submits pursuant to Article 58 (2) (d) i

data protection ordinance Sahlgrenska University Hospital that

1.

ensure that the required needs and risk analysis is carried out and

documented for the journal systems Melior and Nationell

patient overview and that thereafter, with the support of needs and

risk analysis, each user is assigned individual authority for

access to personal data limited to what is

needed for the individual to be able to fulfill his or her duties

in health care, in accordance with Article 5 (1) (f) and Article

32.1 and 32.2 of the Data Protection Ordinance, Chapter 4 § 2 and ch. 6 § 7

the Patient Data Act and Chapter 4 2 § HSLF-FS 2016: 40.

2. document in the journal system Melior's logs so that it appears

what measures have been taken with personal data about a patient, i

in accordance with Article 32 of the Data Protection Ordinance, Chapter 4 § 3

the Patient Data Act and Chapter 4 § 9 (point 1) HSLF-FS 2016: 40.

Report on the supervisory matter

The Data Inspectorate initiated supervision by letter on March 22, 2019 and has

on site on 23 April 2019 reviewed the Board of Sahlgrenska

University Hospital (hereinafter referred to as Sahlgrenska University Hospital)

decisions on the allocation of authorizations have been preceded by a need and

risk analysis. The review has also included how Sahlgrenska

The University Hospital assigned privileges for access to

the main journal system Melior and NPÖ, and what access possibilities they have

granted the privileges provides within the framework of both internal confidentiality

according to ch. 4 the Patient Data Act, as the coherent record keeping according to

Chapter 6 the Patient Data Act. In addition to this, the Data Inspectorate has examined which one

documentation of access (logs) contained in the journal systems.

The Data Inspectorate has only examined users' access possibilities to

the journal system, i.e. what care documentation the user can actually take

part of and read. The supervision has not included which functions were included in

the competence, ie. what the user can actually do in the journal system

(eg issuing prescriptions, writing referrals, etc.).

Previous review of needs and risk analysis

The Data Inspectorate has previously carried out an inspection regarding Sahlgrenska

The university hospital had carried out a documented need and

risk analysis according to ch. Section 6, second paragraph, second sentence of the National Board of Health and Welfare

regulations Information management and record keeping in health care

(SOSFS 2008: 14). Of the Data Inspectorate's decision with record number 1607-2013,

announced on March 27, 2015, it appears that Sahlgrenska University Hospital

did not meet the requirement to carry out a needs and risk analysis according to

said regulations, and was therefore ordered to implement such a

the main journal system.

What has emerged in the case

Sahlgrenska University Hospital has mainly stated the following.

Personal data manager

Sahlgrenska University Hospital has stated that the Board of Sahlgrenska

The University Hospital is responsible for the processing of personal data

personal data that Sahlgrenska University Hospital performs in

the main journal system Melior. Sahlgrenska University Hospital also has

stated that the National Patient Overview (NPÖ) is only a reading view that

presents information from connected systems, and that no information

stored in NPÖ. Sahlgrenska University Hospital is not

personal data controller for information displayed in NPÖ.

Journal system

Sahlgrenska University Hospital has stated that they have been using since 1998
of the main journal system Melior within the framework of internal confidentiality.
Everything is seen as internal secrecy within the framework of the Västra Götaland region.
Since May 6, 2014, Melior in the Västra Götaland region consists of one
single database (GEM), instead of the previous 27. It used to be possible
access other units' care documentation but it was significantly more
cumbersome, which meant that employees were reluctant to read
records of other units. The current division of units is
the same as before but now it is easier to access others
units records.
According to data provided by Sahlgrenska University Hospital
896,401 patients recorded in Melior at Sahlgrenska
University Hospital. The number of employees at Sahlgrenska
The University Hospital is 16,731, and the number of active accounts in Melior is
24 638 st. Sahlgrenska University Hospital has stated that the reason for
that the number of active accounts is greater than the number of employees is that Västra
The Götaland region is an internal privacy zone, and that Sahlgrenska
The University Hospital collaborates with other administrations within Västra
The Götaland region, where employees need access to
patient information at Sahlgrenska University Hospital.
Sahlgrenska University Hospital is not part of a cohesive system
record keeping through Melior, but is included in cohesive record keeping through
the NPÖ system.
Internal secrecy
Needs and risk analysis
At the time of the inspection, Sahlgrenska University Hospital stated in

essentially the following.

When a new employee is hired, a needs analysis is first made, consisting of one

assessment of which systems the employee needs access to.

The assessment is made in two steps: 1) which assignment the person has and 2) which

systems the person needs to have access to in order to perform their

work / assignment. Due to a limitation in the system no one is done

assessment of which tasks in Melior the employee should be able to take part in

of.

Then a risk analysis is made which consists of an assessment at the individual level of

if the person to be assigned eligibility will follow the guidelines for

to take part in information in Melior. If this is not the case, the person should not normally

employed.

At the time of inspection, Sahlgrenska University Hospital cannot present

an analysis for people who are employed and it is unclear whether it is documented.

Sahlgrenska University Hospital has comments on

the inspection report that was received by the Swedish Data Inspectorate on 27 June 2019

stated that Sahlgrenska University Hospital in September 2011 carried out

a comprehensive risk analysis, Availability of the operation of the electronic

the patient record Melior, regarding patient safety, information security and

technical safety. The starting point for the risk analysis at that time was that

simplify access to patient data between the different devices within

the hospital when the National Board of Health and Welfare considered the division into different databases

which was present at the time entailed a patient safety risk. 27 databases

merged into a hospital-wide database and the general role

which is assigned to all staff in need of access to the patient record

was introduced.

Previous review of needs and risk analysis

Due to the Data Inspectorate's previous review, Sahlgrenska has

The University Hospital has submitted a number of documents, including a risk and vulnerability analysis and a so-called

simplified needs and risk analysis with

the title Needs and risk analysis when allocating individual eligibility to

journal systems, which are said to have been developed in the spring of 2019, to show how

Sahlgrenska University Hospital has acted after the inspection earlier

decision.

On 13 September 2019, Sahlgrenska University Hospital was also included

the document Needs and risk analysis for authorization, of which it

states that “In healthcare, the patient's life and health are more important than integrity

which means that accessibility and accuracy outweigh

confidentiality from a patient safety perspective. IN

the patient record system (Melior), the employee must make an active choice for

to be able to access patient information from other care units / processes. We

makes the assessment that that function is sufficient to satisfy

the requirement of confidentiality. We believe it is in accordance with HSLF-FS

2016: 40.

Sahlgrenska University Hospital accepts the risk of

confidentiality is not as high a priority as accuracy and availability

until Sahlgrenska University Hospital has a technical or

organizational opportunity to prioritize confidentiality ”.

Authorization of access to personal data about patients

Sahlgrenska University Hospital has mainly stated the following.

There are two different roles when it comes to assigning reading privileges to

Melior; a general role assigned to all health and medical staff

healthcare, and a so-called operational role.

When it comes to the general role, there are two different variants; a "general"

and a "general including emergency access". All employees within

health care has been assigned a general role - with or without

emergency access.

The difference between the different variants is that the variant “generally inclusive

emergency access ”is assigned to physicians and nurses, and involves the user

has the opportunity to open blocked journals even outside one's own

the activity, in the event that the patient is unable to give his consent.

The "general" variant is assigned to other care staff and secretaries, if desired

say the users who are not doctors or nurses but who should have

eligibility for Melior.

With the general role, the employee has access to all units

care documentation, with the exception of the non-clinical genetics unit

included in the general authorizations. There are no more

restrictions on access in Melior, apart from healthcare documentation such as

the patient himself has blocked.

The business role provides access to blocked information regarding a certain

unit. An employee must have an assignment to be assigned

the business role and can only be assigned that role regarding that unit

to which the employee belongs. Every business has such a business role

and in total the number of such operational roles amounts to about 60-70.

Active choices

During the inspection, Sahlgrenska University Hospital has shown how

the permissions appear in the system, and stated the following, among other things.

When an employee logs in to Melior, he is directed to the unit that

the employee belongs to. When the employee is logged in, there are six tabs in it

the right edge that gives access to different parts of the journal that

the employee has chosen to take part in. As a starting point, only the journal is displayed at

the device that has been selected at login, but through active selections can

the employee has access to other units' records.

If an employee is logged in as a nurse, it is initially only visible

nurses' medical records. However, the employee can get

access to other professional categories' journal entries by checking

boxes for different occupational categories. There is also the opportunity to check

a single box covering all occupational categories, and thereby gaining part of

journal entries of all occupational categories.

Coherent record keeping

Sahlgrenska University Hospital participates in systems for cohesion

record keeping through NPÖ, and has mainly stated the following.

Needs and risk analysis

Sahlgrenska University Hospital has not done any needs and

risk analysis before granting authorization in NPÖ.

Authorization of access to personal data about patients

The patient must be enrolled at Sahlgrenska University Hospital in

Melior so that the employee can use NPÖ.

Access to NPÖ is given to healthcare staff, especially doctors and nurses,

and an employee assignment is required to obtain such authorization. As

As a starting point, only doctors and nurses have access to

NPÖ, but other categories can be accessed upon their own application

competence. In such cases, the employee may apply for an employee assignment

coherent record keeping. The allocation of the authorizations is based on

needs and fewer employees have access to NPÖ than to Melior. For example

assistant nurses need to be able to note in the journal in Melior but they

does not need to have access to NPÖ. Those who are eligible for NPÖ can see all

care documentation available there, but active choices are required.

Documentation of access (logs)

Sahlgrenska University Hospital has stated the following.

The documentation that is displayed when removing the access logs in Melior is

information about the patient, which user has opened the record, which

part of the journal that has been opened and the time and date of the most recent

the opening.

It is not clear at which care unit the measures were taken or which measures

which the user has specifically taken. Sahlgrenska University Hospital has

stated that information about which unit the user is employed on can

controlled by a search on where the user is employed. Different logs

must then be combined with each other.

Justification of the decision

Applicable rules

The Data Protection Regulation is the primary source of law

The Data Protection Regulation, often abbreviated GDPR, was introduced on 25 May 2018 and

is the primary legal regulation in the processing of personal data. This

also applies to health care.

The basic principles for the processing of personal data are set out in

Article 5 of the Data Protection Regulation. A basic principle is the requirement

security pursuant to Article 5 (1) (f), which states that personal data shall be processed

in a way that ensures appropriate security for personal data,

including protection against unauthorized or unauthorized treatment and against loss;

destruction or damage by accident, using appropriate

technical or organizational measures.

Article 5 (2) states the so-called liability, ie. that it

personal data controllers must be responsible for and be able to show that the basics

the principles set out in paragraph 1 are complied with.

Article 24 deals with the responsibility of the controller. Of Article 24 (1)

it appears that the person responsible for personal data is responsible for implementing appropriate

technical and organizational measures to ensure and be able to demonstrate that

the processing is performed in accordance with the Data Protection Regulation. The measures shall

carried out taking into account the nature, scope, context of the treatment

and purposes and the risks, of varying degrees of probability and severity, for

freedoms and rights of natural persons. The measures must be reviewed and updated

if necessary.

Article 32 regulates the security of the processing. According to paragraph 1

the personal data controller and the personal data assistant shall take into account

of the latest developments, implementation costs and treatment

nature, scope, context and purpose as well as the risks, of varying

probability and seriousness, for the rights and freedoms of natural persons

take appropriate technical and organizational measures to ensure a

level of safety appropriate to the risk (…). According to paragraph 2,

when assessing the appropriate level of safety, special consideration is given to the risks

which the treatment entails, in particular from accidental or unlawful destruction,

loss or alteration or to unauthorized disclosure of or unauthorized access to

the personal data transferred, stored or otherwise processed.

Recital 75 states that in assessing the risk to natural persons

rights and freedoms, various factors must be taken into account. Among other things mentioned

personal data covered by professional secrecy, health data or

sexual life, if the processing of personal data concerning vulnerable physical persons takes place

persons, especially children, or if the treatment involves a large number

personal data and applies to a large number of registered persons.

Furthermore, it follows from recital 76 that the likelihood and seriousness of the risk for it

data subjects' rights and freedoms should be determined on the basis of processing

nature, scope, context and purpose. The risk should be evaluated on

on the basis of an objective assessment, which determines whether

the data processing involves a risk or a high risk.

Recitals 39 and 83 also contain writings that provide guidance on it
the meaning of the Data Protection Regulation's requirements for security in
Processing of personal data.

The Data Protection Regulation and the relationship with complementary national
provisions

According to Article 5 (1) (a) of the Data Protection Regulation, personal data must:
treated in a lawful manner. In order for the treatment to be considered legal, it is required
legal basis by at least one of the conditions of Article 6 (1) being met.
The provision of health care is one such task of general
interest referred to in Article 6 (1) (e).
In health care, the legal bases can also be legal
obligation in Article 6 (1) (c) and the exercise of authority under Article 6 (1) (e)
updated.
When it comes to the legal bases legal obligation, in general
interest or exercise of authority by the Member States, in accordance with Article
6.2, maintain or introduce more specific provisions for adaptation
the application of the provisions of the Regulation to national circumstances.
National law may lay down specific requirements for the processing of data
and other measures to ensure legal and fair treatment. But
there is not only one possibility to introduce national rules but also one
duty; Article 6 (3) states that the basis for the treatment referred to in
paragraph 1 (c) and (e) shall be determined in accordance with Union law or
national law of the Member States. The legal basis may also include
specific provision to adapt the application of the provisions of
the Data Protection Regulation. Union law or the national law of the Member States

law must fulfill an objective of general interest and be proportionate to it

legitimate goals pursued.

Article 9 states that the treatment of specific categories of

personal data (so-called sensitive personal data) is prohibited. Sensitive

personal data includes data on health. Article 9 (2) states

except when sensitive personal data may still be processed.

Article 9 (2) (h) states that the processing of sensitive personal data may be repeated

the treatment is necessary for reasons related to, among other things

the provision of health care on the basis of Union law or

national law of the Member States or in accordance with agreements with professionals in

the field of health and provided that the conditions and protective measures provided for in

referred to in paragraph 3 are met. Article 9 (3) requires a regulated duty of confidentiality.

This means that both the legal bases of general interest,

exercise of authority and legal obligation in the treatment of the vulnerable

personal data under the derogation in Article 9 (2) (h)

supplementary rules.

Supplementary national regulations

In the case of Sweden, both the basis for the treatment and those

special conditions for the processing of personal data in the field of health and

healthcare regulated in the Patient Data Act (2008: 355), and

the Patient Data Ordinance (2008: 360). I 1 kap. Section 4 of the Patient Data Act states that

the law complements the data protection regulation.

The purpose of the Patient Data Act is to provide information in health and

healthcare must be organized so that it meets patient safety and

good quality and promotes cost efficiency. Its purpose is also to

personal data shall be designed and otherwise processed so that patients and

the privacy of other data subjects is respected. In addition, must be documented

personal data is handled and stored so that unauthorized persons do not have access to it

them (Chapter 1, Section 2 of the Patient Data Act).

According to ch. Section 6 of the Patient Data Act is a care provider responsible for personal data

for the processing of personal data carried out by the care provider. In a region

and one municipality is each authority that conducts health and medical care

personal data controller for the processing of personal data that

the authority performs.

The supplementary provisions in the Patient Data Act aim to:

take care of both privacy protection and patient safety. The legislator has

thus through the regulation made a balance in terms of how

the information must be processed to meet both the requirements for patient safety

as the right to privacy in the processing of personal data.

The National Board of Health and Welfare has, with the support of the Patient Data Ordinance, issued regulations

and general advice on record keeping and processing of personal data in

health care (HSLF-FS 2016: 40). The regulations constitute such

supplementary rules, which shall be applied in the care provider's treatment of

personal data in health care.

National provisions that supplement the requirements of the Data Protection Regulation

security can be found in Chapters 4 and 6. the Patient Data Act and Chapters 3 and 4 HSLF-FS

2016: 40.

Requirement to do needs and risk analysis

According to ch. 4, the care provider must § 2 HSLF-FS 2016: 40 make a needs and

risk analysis, before the allocation of authorizations in the system takes place.

That both the needs and the risks are required is clear from the preparatory work

to the Patient Data Act, prop. 2007/08: 126 pp. 148-149, as follows.

Authorization for staff's electronic access to patient information shall be restricted to

what the executive needs to be able to perform his duties in health and

healthcare. This includes that authorizations should be followed up and changed or restricted accordingly

hand as changes in the tasks of the individual executive give rise to it.

The provision corresponds in principle to section 8 of the Health Care Register Act. The purpose of the provision is to

imprint the obligation on the responsible caregiver to make active and individual

eligibility assignments based on analyzes of which details are different

staff categories and different types of activities need. But it's not just needed

needs analyzes. Risk analyzes must also be done where different types of risks are taken into account, such as

may be associated with an overly availability of certain types of information.

Protected personal data that is classified, information about publicly known persons,

data from certain clinics or medical specialties are examples of categories such as

may require special risk assessments.

In general, it can be said that the more comprehensive an information system is, the greater the amount

there must be different levels of eligibility. Decisive for decisions on eligibility for e.g. various

categories of healthcare professionals for electronic access to data in

patient records should be that the authority should be limited to what the executive needs

for the purpose a good and safe patient care. A more extensive or coarse-meshed

allocation of competence should - even if it has points from the point of view of efficiency - be regarded as an unjustified

dissemination of medical records within an

not accepted.

Furthermore, data should be stored in different layers so that more sensitive data require active choices or otherwise not as easily accessible to staff as less sensitive tasks. When it applies to staff who work with business follow-up, statistics production, central financial administration and similar activities that are not individual-oriented, it should be most executives have enough access to information that can only be indirectly derived to individual patients. Electronic access to code keys, social security numbers and others data that directly point out individual patients should be strong in this area limited to individuals.

Internal secrecy

The provisions in ch. 4 The Patient Data Act concerns internal confidentiality, ie. regulates how privacy protection is to be handled within a care provider's business and in particular employees' opportunities to prepare for access to personal data that is electronically available in a healthcare provider organisation.

It appears from ch. Section 2 of the Patient Data Act stipulates that the care provider must decide conditions for granting access to such data patients who are fully or partially automated. Such authorization shall limited to what is needed for the individual to be able to fulfill theirs tasks in health care.

According to ch. 4 § 2 HSLF-FS 2016: 40, the care provider shall be responsible for each users are assigned an individual privilege to access personal data. The caregiver's decision on the allocation of eligibility shall

preceded by a needs and risk analysis.

Coherent record keeping

The provisions in ch. 6 the Patient Data Act concerns cohesive record keeping,

which means that a care provider - under the conditions specified in § 2 of the same

chapter - may have direct access to personal data processed by others

caregivers for purposes related to care documentation. The access to

information is provided by a healthcare provider making the information about a patient

which the care provider registers if the patient is available to other care providers

who participate in the coherent record keeping (see Bill 2007/08: 126 p. 247).

Of ch. 6 Section 7 of the Patient Data Act follows that the provisions in Chapter 4 § 2 also

applies to authorization allocation for unified record keeping. The requirement of

that the care provider must perform a needs and risk analysis before allocating

permissions in the system take place, also applies in systems for cohesion

record keeping.

Documentation of access (logs)

Of ch. 4 Section 3 of the Patient Data Act states that a care provider must ensure that

access to such data on patients kept in whole or in part

automatically documented and systematically checked.

According to ch. 4 Section 9 HSLF-FS 2016: 40, the care provider shall be responsible for that

1.

it appears from the documentation of the access (logs) which

measures taken with information on a patient,

2. it appears from the logs at which care unit or care process

measures have been taken,

3. the logs indicate the time at which the measures were taken;

4. the identity of the user and the patient is stated in the logs.

The Data Inspectorate's assessment

Responsibility of the data controller for security

As described above, the National Board of Health and Welfare's regulations give the caregiver one responsibility for information management in healthcare, such as that carry out a needs and risk analysis before assigning authorizations in the system happens. In public health care does not coincide always the concept of caregiver with the personal data controller.

Of both the basic principles of Article 5 and Article 24 (1) the Data Protection Ordinance, it appears that it is the person responsible for personal data which shall implement appropriate technical and organizational measures to: ensure and be able to demonstrate that the treatment is carried out in accordance with the Data Protection Regulation.

The Data Inspectorate can state that the Data Protection Ordinance in its capacity as EU regulation is directly applicable in Swedish law and that in the regulation indicates when supplementary regulation is or may be introduced nationally. There is for example, space to nationally regulate who is data controller in accordance with Article 4 of the Data Protection Regulation. It is however, it is not possible to give deviating regulation regarding it the responsibility of the data controller to take appropriate technical and organizational measures to ensure an appropriate level of security in relation to the risk. This means that the National Board of Health and Welfare's regulations state that it is the caregiver who must take certain measures, does not change that the responsibility to take appropriate security measures rests with it

personal data controller according to the Data Protection Regulation. The Data Inspectorate can state that Sahlgrenska University Hospital, in its capacity as responsible for personal data, is responsible for taking these measures.

As previously described, Article 24 (1) of the Data Protection Regulation provides a general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement is partly to ensure that the processing of personal data is carried out in accordance with the Data Protection Ordinance, and that the data controller must be able to demonstrate that the processing of personal data is carried out in accordance with the Data Protection Regulation.

The safety associated with the treatment is regulated more specifically in the articles 5.1 f and 32 of the Data Protection Regulation.

Article 32 (1) states that the appropriate measures shall be both technical and organizational and they must ensure a level of security appropriate in in relation to the risks to the rights and freedoms of natural persons which the treatment entails. It is therefore necessary to identify the possible ones the risks to the data subjects' rights and freedoms and assess the probability of the risks occurring and the severity if they occur.

What is appropriate varies not only in relation to the risks but also based on the nature, scope, context and purpose of the treatment. It has thus the significance of what personal data is processed, how many data, it is a question of how many people process the data, etc.

The health service has a great need for information in its operations. The

It is therefore natural that the possibilities of digitalisation are utilized as much as possible in healthcare. Since the Patient Data Act was introduced, a lot extensive digitization has taken place in healthcare. Both the data collections size as the number of people sharing information with each other has increased substantially. At the same time, this increase means that the demands on it increase personal data controller, as the assessment of what is an appropriate safety is affected by the extent of the treatment.

It is also a question of sensitive personal data. The information concerns people who are in a situation of dependence when they are in need of care.

It is also often a question of a lot of personal information about each of these people and the data may over time be processed by very many people in healthcare. All in all, this places great demands on it personal data controller.

The data processed must be protected from outside actors as well the business as against unauthorized access from within the business. It appears of Article 32 (2) that the data controller, in assessing the appropriate

level of security, in particular to take into account the risks of unintentional or illegal destruction, loss or for unauthorized disclosure or unauthorized access. In order to be able to know what is an unauthorized access it must personal data controllers must be clear about what an authorized access is.

Needs and risk analysis

I 4 kap. Section 2 of the National Board of Health and Welfare's regulations (HSLF-FS 2016: 40) which supplement In the Patient Data Act, it is stated that the care provider must make a needs and

risk analysis before the allocation of authorizations in the system takes place. This means that

national law prescribes requirements for an appropriate organizational measure that shall:

taken before the allocation of permissions to the journal system takes place.

A needs and risk analysis must include an analysis of the needs and a

analysis of the risks from an integrity perspective that may be associated

with an overly allotment of access to personal data

about patients. Both the needs and the risks must be assessed on the basis of them

tasks that need to be processed in the business, what processes it is

the question of whether and what risks to the privacy of the individual exist.

The assessments of the risks need to be made on the basis of organizational level, there

for example, a certain business part or task may be more

more sensitive to privacy than another, but also based on the individual level, if any

the question of special circumstances that need to be taken into account, such as

that it is a question of protected personal data, publicly known persons or

otherwise particularly vulnerable persons. The size of the system also affects

the risk assessment. The preparatory work for the Patient Data Act shows that the more

comprehensive an information system is, the greater the variety

eligibility levels must exist. (Prop. 2007/08: 126 p. 149). It is thus

the question of a strategic analysis at the strategic level, which should provide one

authorization structure that is adapted to the business and this must be maintained

updated.

In summary, the regulation requires that the risk analysis identify

-

different categories of data (eg health data),

-

categories of data subjects (eg vulnerable natural persons and

children), or

-

the scope (eg number of personal data and registered)

-

negative consequences for data subjects (eg damages,

significant social or economic disadvantage, deprivation of rights

and freedoms),

and how they affect the risk to the rights and freedoms of natural persons

Processing of personal data. This applies to both internal secrecy

as in coherent record keeping.

The risk analysis must also include special risk assessments, for example

based on whether there is protected personal data that is

classified, information on public figures, information from

certain clinics or medical specialties (Bill 2007/08: 126 p. 148149).

The risk analysis must also include an assessment of how probable and serious

the risk to the data subjects' rights and freedoms is and in any case determined

whether it is a risk or a high risk (recital 76).

It is thus through the needs and risk analysis that it

personal data controller finds out who needs access, which

information the accessibility shall include, at what times and at what

context access is needed, while analyzing the risks to it

the freedoms and rights of the individual that the treatment may lead to. The result should

then lead to the technical and organizational measures needed to

ensure that no access other than that of need and

the risk analysis shows that it is justified to be able to do so.

When a needs and risk analysis is missing prior to the allocation of eligibility in

system, lacks the basis for the personal data controller on a legal

be able to assign their users a correct authorization. The

the data controller is responsible for, and shall have control over, the

personal data processing that takes place within the framework of the business. To

assign users one upon access to journal system, without this being founded

on a performed needs and risk analysis, means that the person responsible for personal data

does not have sufficient control over the personal data processing that takes place in

the journal system and also can not show that he has the control that

required.

Sahlgrenska University Hospital's process for needs and risk analysis

Sahlgrenska University Hospital has within the framework of the supervisory matter

referred to three different processes or documents that are said to constitute one

needs and risk analysis. Regarding the process that Sahlgrenska

The university hospital referred to at the time of the inspection passed this

partly in an assessment of which assignments the person has and which systems

the person needs to have access to, partly in an assessment at the individual level of whether

the employee who was to be hired seemed inclined to take part in tasks

in the medical record system in violation of current guidelines.

The Data Inspectorate can state that Sahlgrenska University Hospital does not

has carried out an analysis relating to the business, various processes and

the need for staff categories to process data. What is described is

instead, only an assessment of what systems an employee needs to have

access to.

The risk analysis described by Sahlgrenska University Hospital is about one

risk assessment other than that referred to in the National Board of Health and Welfare's regulations. IN

the needs and risk analysis, risks to the individual's integrity must be identified.

As is clear from the preparatory work for the Patient Data Act, certain information may be required

special risk assessment and protected personal data are given as examples

which are classified, information about publicly known persons, information

from certain clinics or medical specialties. So it is not

the assessment of the employee referred to in this context. On the contrary have

the legislator emphasizes precisely that even if health care should be able to have large

trust in their employees, it is not in itself sufficient protection,

The ethical principle of confidentiality is deeply rooted in health care

information that emerges in the contact between health care professionals and patients

is obviously a strong counterforce against gossiping about patients or otherwise spreading information

in an unacceptable way among co-workers. The same is true of the tendency to

find out information about patients who are cared for in the workplace but who do not have one themselves

professional relationship to. Given the scope of health care and the big picture

the number of employed health and medical staff, about 300,000 people in the municipalities alone

and the county council's health and medical care, however, it cannot be assumed that this is not the case at all

occurs.

The development towards common widely available electronic journal systems within the large ones

At the same time, the care providers' operations entail increased risks of invasion of privacy. If it increased

potential availability of medical records is not handled in a good way so that patients

can feel confident that sensitive information is not read by unauthorized persons, there is a great risk

that patients choose to stay out of electronic access systems.

A mixture of preventive and reactive measures is needed to prevent patient data

shall be handled in an unacceptable manner (Bill 2007/08: 126 pp. 147-147).

The process that Sahlgrenska described at the time of the inspection is

thus not a needs and risk analysis according to ch. 2 § HSLF-FS 2016: 40.

The document Availability for operation of the electronic patient record

Melior

Sahlgrenska University Hospital has in supplementary information that

received by the Swedish Data Inspectorate on 27 June 2019 stated that the document

Accessibility to the operation of the electronic patient record Melior constitutes one

needs and risk analysis. The document is stated to have been drawn up in 2011 and to have as

starting point to simplify access to patient data between the different

the units within the hospital. However, it can be stated that by

the document states that it aims to carry out a risk analysis regarding

operation of the Melior medical record system. In the section “Risk identification and

underlying causes "the identified risks are attributed either to" Part 1:

Patient safety and operational perspective ”or“ Part 2: Technical safety

with regard to availability for operation ”.

Regarding the needs analysis, the document does not contain an analysis of which ones

tasks employees need to be able to perform their

tasks. Regarding the risk analysis, examples of risks are as

identified in Part 1: Patient safety and operational perspective that "All IT-related deviations that may affect patient safety are

not reported",

or "Wrong patient is dictated to the wrong dictation". Risks identified in Part 2:

Technical safety with regard to availability for operation, is for example “unauthorized

access to journal information ”, caused by“ transmission via

open networks ”. There are risks from an information security perspective, however

the document does not contain any analysis of the risks that may be associated

with an overly wide availability regarding different types of personal data.

The document is thus an analysis from a business perspective and fulfills

not the requirements for a needs and risk analysis from an integrity perspective according to 4

Cape. 2 § HSLF-FS 2016: 40.

The document risk and vulnerability analysis

Sahlgrenska University Hospital also has due to

The Data Inspectorate's inquiry as to what measures have been taken after

the authority's decision 1607-2013, in which Sahlgrenska University Hospital

was instructed to produce a documented needs and risk analysis, stated that

In the spring of 2019, a needs and risk analysis was carried out. Sahlgrenska

The University Hospital has submitted three different documents, a risk and

vulnerability analysis, a so-called simplified needs and risk analysis with the title

Needs and risk analysis when allocating individual eligibility to

journal system, and a document entitled Needs and risk analysis at

authorization allocation which can be said to constitute a brief account of how

the other two documents are used in the business. Initially, it can

It is noted that the documents were not produced until four years after the Data Inspectorate

order. In addition, none of the submitted documents constitutes a needs and risk analysis from an integrity perspective.

Regarding the risk and vulnerability analysis, it is an analysis that must be performed according to the legislation on heightened preparedness and crisis preparedness2. Such a thing happens for other purposes and is not the same as a needs and risk analysis according to in ch. 4 2 § HSLF-FS 2016: 40.

It appears from the risk and vulnerability analysis that a measure to deal with one too at the level of eligibility should be to implement a simplified needs and risk analysis when allocating eligibility. The document thus states that a needs and risk analysis must be done, but does not in itself constitute one.

The document does not contain an analysis of what tasks the employees have need in the journal system to be able to perform their tasks. The there are parts that concern the risk to the individual's integrity, but the so-called identified consequences do not constitute an analysis of risks in the current case case but rather a statement of facts, such as that of a consequence that the internal area of confidentiality is extensive is that “VGR has many employee which can lead to the permissions becoming too wide, which gives employees more competence than they need ”. In some parts contains the document identified risks which, however, do not aim at the protection of the integrity of the individual; for example, it is found that a consequence of that employees do not know what applies when accessing patient data is that “patients when requesting a log extract can see that an unauthorized person has looked in journal, bad will for SU ”.

Act (2006: 544) on municipalities 'and county councils' measures before and during extraordinary events in peacetime and heightened preparedness, ordinance (2015: 1052) on crisis preparedness and measures by the authorities responsible for surveillance in the event of heightened preparedness.

2

In summary, the Data Inspectorate can state that the document does not

contains analyzes of the need for access to personal data or the risks

for the integrity of the individual arising from an excessively wide

authorization, and thus does not meet the requirements of a needs and

risk analysis from an integrity perspective according to ch. 2 § HSLF-FS 2016: 40.

The simplified needs and risk analysis

Regarding the simplified needs and risk analysis that Sahlgrenska determines in the risk and vulnerability analysis to be made

when allocating eligibility,

it is initially stated that it is not compatible with in ch. § 2 HSLFFS 2016: 40 to only perform a simplified needs and risk

analysis. Further

the document consists of a list of 14 questions to be answered with yes or

no, such as “the employee knows that the computer must not be left unlocked,

without supervision? ”. The Data Inspectorate can state that this is rather a question of

a document to be used to create the conditions for a good

information security at the individual level. It's an organizational measure to

ensure an appropriate level of security, but it is not an analysis of the need for

access to personal data or what risks to the privacy of the individual

arises through an overly authoritative control. Thus does not meet

nor does this document the requirements of a needs and risk analysis from a

integrity perspective according to ch. 4 2 § HSLF-FS 2016: 40.

The document Needs and risk analysis when allocating eligibility

Sahlgrenska University Hospital has also submitted a document in which

the work with needs and risk analysis is briefly described. The document

briefly describes how the risk and vulnerability analysis and the simplified one

the needs and risk analysis is used in the business, and how Sahlgrenska

The university hospital prioritizes accuracy and accessibility over

confidentiality. The document does not contain any analyzes of the need for access

to personal data or the risks to the privacy of the individual that

arises through an overly in allocation of eligibility, and meets

thus not the requirements for a needs and risk analysis according to ch. § 2 HSLF-FS

2016: 40. Instead, the document shows that Sahlgrenska University Hospital

deliberately prioritizes the requirement of confidentiality.

The Swedish Data Inspectorate's summary assessment

As stated above, in a needs and risk analysis, both the needs and

the risks are assessed on the basis of the data that need to be processed in

the business, what processes are involved and what are the risks for it

individual integrity that exists on both organizational and individual

level. It is thus a question of a strategic analysis at a strategic level, which

shall provide an authorization structure that is adapted to the business. It should

result in authorization assignments but it is not

the instructions to the person who assigns the permissions that are the analysis.

At the Data Inspectorate's review, Sahlgrenska University Hospital has

have not been able to present any needs and risk analysis within the framework of

internal secrecy or within the framework of the cohesive

record keeping. Sahlgrenska University Hospital's document lacks it

basic inventory of users' access and analysis needs

of risks, nor has any balance been made between needs and those

actual privacy risks that the processing of personal data gives rise to.

In summary, the Data Inspectorate can state that the documents that

have not been reported individually or together meet the requirements

on a needs and risk analysis and that Sahlgrenska University Hospital does not

have been able to show that they have carried out a needs and risk analysis in that sense

as referred to in ch. 4 § 2 HSLF-FS 2016: 40, neither within the framework of the internal

secrecy or within the framework of the unified record keeping, according to 4

respectively 6 chap. the Patient Data Act. This means that Sahlgrenska

The University Hospital has not taken appropriate organizational measures in

in accordance with Article 5 (1) (f) and Article 31 (1) and (2) in order to ensure and,

in accordance with Article 5 (2), be able to demonstrate that the processing of personal data

have a security that is appropriate in relation to the risks.

Authorization of access to personal data about patients

As reported above, a caregiver may have a legitimate interest in having

a comprehensive processing of data on the health of individuals. Notwithstanding this shall

access to personal data about patients may be limited to

what is needed for the individual to be able to fulfill his or her duties.

With regard to the allocation of authorization for electronic access according to ch.

§ 2 and ch. 6 Section 7 of the Patient Data Act states in the preparatory work, Bill.

2007/08: 126 pp. 148-149, i.a. that there should be different eligibility categories in

the journal system and that the permissions should be limited to what the user

need to provide the patient with good and safe care. It also appears that “a

more extensive or coarse-grained eligibility should be considered as one

unauthorized dissemination of journal information within a business and should as

such is not accepted. "

In health care, it is the person who needs the information in their work

who may be authorized to access them. This applies both within a

caregivers as between caregivers. It is, as already mentioned, through

the needs and risk analysis that the person responsible for personal data finds out who

who need access, what information the access should include, at which

times and in which contexts access is needed, and at the same time

analyzes the risks to the individual's freedoms and rights

the treatment can lead to. The result should then lead to the technical and

organizational measures needed to ensure no allocation

of eligibility provides further access opportunities than the one that needs and

the risk analysis shows is justified. An important organizational measure is to provide

instruction to those who have the authority to assign permissions on how this

should go to and what should be considered so that it, with the needs and risk analysis

as a basis, becomes a correct authorization allocation in each individual case.

As emerged in the case, about 900,000 patients are registered in Melior at

Sahlgrenska University Hospital and the number of active accounts in Melior are

close to 25,000, which exceeds the number of employees at Sahlgrenska

The University Hospital, which at the time of the inspection was close to 18,000.

Sahlgrenska University Hospital has assigned the employees who work

with health care a general eligibility role - with or without

emergency access - which provides access to all units' care documentation,

with the exception of the clinical genetics unit which is not included in the

general competences. Thus, the majority of users have actually had

access to most of this information. This means that

Sahlgrenska University Hospital does not have a sufficient extent

restricted users' permissions to access personal data about

patients in the Melior medical record system.

In addition, it can be stated that Sahlgrenska University Hospital has given

direct access to personal data about patients at Sahlgrenska

The University Hospital for employees at other administrations in Västra

Götaland region.

Access to personal data in Melior presupposes that the user is active

choice. Sahlgrenska University Hospital has stated that they assess that

the active selection function is sufficient to meet the requirement of confidentiality

and that it is in accordance with HSLF-FS 2016: 40. The Data Inspectorate can

however, note that the Patient Data Act requires both limitation

of competencies and active choices. The active selection function is therefore not a measure

to compensate for a lack of access restriction. That Sahlgrenska

The University Hospital uses the above active choices is one

privacy enhancing measure, but does not constitute such a restriction of

competence referred to in ch. 4 Section 2 of the Patient Data Act. This provision

requires that the authority be limited to what is needed for it

individuals must be able to fulfill their duties in health care,

i.e. only those who need the information should have access to

them.

Of the preparatory work for the Patient Data Act, Bill. 2007/08: 126, p. 149, it appears that

the purpose of the provisions is to imprint the obligation on the person responsible

the caregiver to make active and individual eligibility allocations from outside

analyzes of which details information different staff categories and different

kind of activities need. Because different users have different

tasks in different work areas, users need access to

the data in Melior is limited to reflect this. Of the preparatory work

it also appears that data should be stored in different layers so that more sensitive

tasks require active choices or are otherwise not as easily accessible

staff as less sensitive tasks.

That the allocation of authorizations has not been preceded by a need and

risk analysis means that Sahlgrenska University Hospital has not analyzed

users' need for access to the data, the risks associated with that access

can entail and thus also not identified which access is

justified to users on the basis of such an analysis. Sahlgrenska

The University Hospital has thus not used appropriate measures, in

in accordance with Article 32, to restrict users' access to

patients' data in the medical record system.

Regarding the processing of personal data by Sahlgrenska

The university hospital performs within the framework of the cohesive

record keeping in the NPÖ system, it can initially be stated that

Sahlgrenska University Hospital has stated that Sahlgrenska

The University Hospital is not responsible for that information

shown in NPÖ. The Data Inspectorate does not share this view. According to 2

Cape. Section 6 of the Patient Data Act In a region, each authority that conducts health and medical care is responsible for the

processing of personal data.

carried out by the authority. According to the second paragraph of the provision covers

personal data liability also such processing of personal data as

the care provider, or the authority in a region or municipality that is

personal data controller, performs when the care provider or authority through

direct access in an individual case prepares access to personal data about a

patient with another care provider or other authority in the same region or

municipality. Sahlgrenska University Hospital is thus

personal data controller for the processing of personal data that takes place when

the employees take part in tasks in NPÖ.

With regard to access to personal data within the framework of it

cohesive record keeping in the NPÖ system has about 7,000 users

Sahlgrenska University Hospital access. The Data Inspectorate can

note that there has been a restriction on the number of users in

compared to the approximately 25,000 who have eligibility in Melior, but do not

any restriction has been made as to what documentation these are

users can take part in the NPÖ system.

This in turn has meant that there has been a risk of unauthorized access and

unjustified dissemination of personal data partly within the framework of the internal

secrecy, partly within the framework of the coherent record keeping.

In the light of the above, the Data Inspectorate can state that

Sahlgrenska University Hospital has processed personal data in violation of

Article 5 (1) (f) and Article 32 (1) and (2) of the Data Protection Regulation by

Sahlgrenska University Hospital has not restricted users

permissions for accessing the Melior journal system to what only

is needed for the user to be able to fulfill his tasks within

health and medical care according to ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and 4

Cape. 2 § HSLF-FS 2016: 40. This means that Sahlgrenska

The University Hospital has not taken measures to ensure and,

in accordance with Article 5 (2) of the Data Protection Regulation, be able to demonstrate an appropriate

security of personal data.

Documentation of access (logs)

The Data Inspectorate can state that the logs showing access in Melior

contains information about the user's name and role, patients' identities,

which part of the journal has been opened (eg journal, referrals, certificate - someone

of the "six tabs") and the date and time the measures were taken.

It is not clear at which care unit the measure was taken or which ones

actions specifically taken by the user. Sahlgrenska has stated that

information about which care unit the user is employed at can be checked

through a search on where the user is employed. Sahlgrenska therefore means

that by combining different logs, you can find out at which care unit

as the measure has been taken. Each log entry in the logs constitutes the action “open

journal". In addition, it is not clear what actions the user has

taken with information about a patient.

Sahlgrenska University Hospital has in an opinion received

The Data Inspectorate on 17 March 2020 stated that the measures set out in

the logs are if an employee has opened the journal, about access to information

occurred through active selection and if the employee from the journal has made one

outreach to other care units. Sahlgrenska University Hospital states

further that the documentation in the logs creates conditions for

perform access controls in an appropriate manner, and that the logs

meets the requirement to log which measures have been taken with information

about a patient.

It appears from the National Board of Health and Welfare's Handbook when applying

The National Board of Health and Welfare's regulations and general guidelines (HSLF-FS 2016: 40) that

“The care provider is responsible, among other things, for the documentation of

the access (logs) shows the measures that have been taken with information

about a patient. An active choice to access information about a patient is

an example of an action to be logged ”.

The Data Inspectorate states that the purpose of the requirement that action be taken

documented in the logs is not just about checking on an employee

prepared access to the journal, but also what measures have been taken with

information about a patient. The action documented in the logs “open

journal ”is an example of an action that should be logged, and in addition should also

other measures taken with information about a patient are documented in

the logs. Other such measures may include the creation of personal data,

copied, transferred, blocked, shredded or printed. the purpose with

The security measure logs are to answer the question of who did what, it wants

say who took what action, with what personal information and when. This

constitutes an important part for the person responsible for personal data to fulfill the requirement for

appropriate security measures to control personal data; and

how they are treated. The purpose of the access control security measure is to

ensure that users do not misuse their permissions through

to read, change or delete information that they should not process. To

Sahlgrenska University Hospital only introduced documentation of the measure

"Open journal", is thus not sufficient to meet the requirement in ch. § 9

(point 1) HSLF-FS 2016: 40 that the documentation of the access should

state what measures have been taken with information about a patient.

Sahlgrenska University Hospital has thus treated and is treating

personal data in violation of ch. 4 Section 3 of the Patient Data Act and Chapter 4 § 9 (point

1) HSLF-FS 2016: 40. This means that Sahlgrenska University Hospital does not

have taken appropriate technical and organizational measures in

relation to the risk. Sahlgrenska University Hospital thus fulfills

not the requirement to ensure adequate security for the processing of

personal data, in accordance with Article 32 of the Data Protection Regulation.

Choice of intervention

Legal regulation

If there has been a violation of the Data Protection Regulation

The Data Inspectorate a number of corrective powers available under the article

58.2 a – j of the Data Protection Regulation. The supervisory authority can, among other things

instruct the person responsible for personal data to ensure that the processing takes place in

in accordance with the Regulation and if required in a specific way and within a

specific period.

It follows from Article 58 (2) of the Data Protection Ordinance that the Data Inspectorate in

in accordance with Article 83 shall impose penalty charges in addition to or in lieu of

other corrective measures referred to in Article 58 (2),

the circumstances of each individual case.

For authorities, according to Article 83 (7) of the Data Protection Regulation, national

rules state that authorities may be subject to administrative penalty fees.

According to ch. 6 Section 2 of the Data Protection Act allows for penalty fees to be decided

authorities, but to a maximum of SEK 5,000,000 or SEK 10,000,000

depending on whether the infringement concerns articles covered by Article 83 (4)

or 83.5 of the Data Protection Regulation.

Article 83 (2) of the Data Protection Regulation sets out the factors to be taken into account

to decide whether to impose an administrative penalty fee, but also

what is to affect the size of the penalty fee. Of central importance to

the assessment of the gravity of the infringement is its nature, severity and

duration. In the case of a minor infringement may

the supervisory authority, in accordance with recital 148 of the Data Protection Regulation, issue a

reprimand instead of imposing a penalty fee.

Order

As mentioned, the health service has a great need for information in its

operations and in recent years has a very extensive digitization

occurred in healthcare. Both the data collections size and how many

sharing information with each other has increased significantly. This increases the demands on

the person responsible for personal data, as the assessment of what is appropriate

safety is affected by the extent of the treatment.

In health care, this means that a great deal of responsibility rests on it

personal data controller to protect the data from unauthorized access,

among other things by having an authorization allocation that is even more

comminuted. It is therefore essential that there is a real analysis of the needs

based on different activities and different executives. Equally important is that

there is an actual analysis of the risks from an integrity perspective

may occur in the event of an override of access rights. From

this analysis must then be restricted to the individual executive.

This authority must then be followed up and changed or restricted accordingly

hand that changes in the individual executive's duties

reason for it.

The Data Inspectorate's inspection has shown that Sahlgrenska University Hospital

have not taken appropriate security measures to provide protection to

the personal data in the record system by Sahlgrenska

University hospital in its capacity as data controller did not comply with the requirements

which is set in the Patient Data Act and the National Board of Health and Welfare's regulations. Sahlgrenska

The University Hospital has thereby failed to comply with the requirements of Article 5 (1) (f)

and Article 32 (1) and (2) of the Data Protection Regulation. The omission includes

both the internal secrecy according to ch. the Patient Data Act as it

coherent record keeping according to ch. 6 the Patient Data Act.

The Data Inspectorate therefore submits pursuant to Article 58 (2) (d) i

data protection ordinance Sahlgrenska University Hospital to ensure that

required needs and risk analysis is performed and documented for

medical records systems Melior and National Patient Overview and that thereafter, with

support of the needs and risk analysis, each user is assigned individually

authorization for access to personal data that is limited to what only

necessary for the individual to be able to fulfill his duties within

health care, in accordance with Article 5 (1) (f) and Article 32 (1) and (2) (i)

the Data Protection Ordinance, Chapter 4 § 2 and ch. 6 Section 7 of the Patient Data Act and 4

Cape. 2 § HSLF-FS 2016: 40.

Sahlgrenska University Hospital has also failed to log in Melior

indicate what measures have been taken with information about a patient, a requirement

which appears from ch. 4 Section 3 of the Patient Data Act and Chapter 4 § 9 (item 1) HSLF-FS

2016: 40. The Data Inspectorate therefore submits Sahlgrenska

The University Hospital to introduce documentation in the logs in Melior where it

shall state what measures have been taken with personal data about one

patient according to ch. 4 Section 3 of the Patient Data Act and Chapter 4 § 9 (item 1) HSLF-FS

2016: 40.

Penalty fee

The Data Inspectorate can state that the violations are fundamentally related

Sahlgrenska University Hospital's obligation to take appropriate

security measures to provide protection of personal data according to

the Data Protection Regulation.

In this case, it is a matter of large collections of data with sensitive

personal data and extensive powers. The caregiver needs to be involved

necessity to have a comprehensive processing of data on the health of individuals.

However, it must not be unrestricted but should be based on what individual

employees need to be able to perform their tasks. The Data Inspectorate

notes that this is information that includes direct identification

by the individual through name, contact information and social security number,

information about health, but that it may also be about other private

information about, for example, family relationships, sexual life and lifestyle. Patients

is dependent on receiving care and is thus in a vulnerable situation. The data

nature, scope and patients' dependence give caregivers a

special responsibility to ensure patients' right to adequate protection for their

personal data.

Additional aggravating circumstances are the treatment of

personal data about patients in the main medical record system belongs to the core of a

the activities of caregivers, that the treatment covers many patients and that

the possibility of access refers not only to a large proportion of employees but to

Sahlgrenska University Hospital has also provided access to a large number

employees at other administrations within the Västra Götaland region. In this

In this case, there are around 900,000 patients within the internal framework

confidentiality, close to 18,000 employees and 25,000 active accounts. There is

only one unit, the unit for clinical genetics, where the data is not accessible

for users outside these devices because the device is excluded from

the general competencies.

The Data Inspectorate can also state that Sahlgrenska

The University Hospital has not complied with the Data Inspectorate's decision of 27

March 2015. In the decision, Sahlgrenska University Hospital was instructed to

carry out a documented needs and risk analysis according to the then

requirement 2 chap. § 6 second paragraph second sentence SOSFS 2008: 14, which

corresponds to the current provision in ch. 4 2 § HSLF-FS 2016: 40. This is a

aggravating circumstance, in accordance with Article 83 (2) (e) of the Data Protection Regulation.

The shortcomings that have now been established have thus been known to Sahlgrenska

the university hospital for several years, which means that the action took place

intentionally and thus is considered more serious.

The Data Inspectorate also states that Sahlgrenska University Hospital in

information received in the case has stated that the care provider accepts

the risk that confidentiality is not given as high a priority as accuracy and

availability. As the Data Inspectorate understands, Sahlgrenska has

The University Hospital has actively taken a position to prioritize taking away

measures to protect the privacy of the individual, making the action

more serious.

Taken together, these factors mean that the infringements are not to be assessed

as minor violations without violations that should lead to a

administrative penalty fee.

The Data Inspectorate considers that the violations are closely related to

each other. That assessment is based on the need and risk analysis

form the basis for the allocation of the authorizations. The Data Inspectorate

therefore considers that these infringements are so closely linked

that they constitute interconnected data processing within the meaning of Article 83 (3) (i)

the Data Protection Regulation. The Data Inspectorate therefore decides on a joint

penalty fee for the infringements.

Regarding the shortcomings in the logs, the Data Inspectorate can state that not

all the information that should be included in the logs does so, but that logging essentially

contains the information required by the National Board of Health and Welfare's regulations.

The Data Inspectorate therefore considers it sufficient that Sahlgrenska

The university hospital is ordered to rectify the shortcoming and therefore does not decide

any special penalty fee for this violation.

The administrative penalty fee shall be effective, proportionate and

deterrent. This means that the amount must be determined so that it

the administrative penalty fee leads to correction, that it provides a preventive

effect and that it is also proportional in relation to both current

violations as to the ability of the supervised entity to pay.

The maximum amount for the penalty fee in this case is SEK 10 million

according to ch. 6 Section 2 of the Act (2018: 218) with supplementary provisions to the EU

data protection regulation.

In view of the seriousness of the infringements and that the administrative

the penalty fee must be effective, proportionate and dissuasive

the Data Inspectorate determines the administrative sanction fee for

Sahlgrenska University Hospital to 3,500,000 (three million five hundred

thousand crowns.

This decision was made by the Director General Lena Lindgren Schelin after

presentation by the IT security specialist Magnus Bergström. At the final

The case is handled by Hans-Olof Lindblom, General Counsel, and the Heads of Unit

Malin Blixt and Katarina Tullstedt participated.

The Data Inspectorate

DI-2019-3840

Lena Lindgren Schelin, 2020-12-02 (This is an electronic signature)

Appendices: Appendix 1 - How to pay a penalty fee

Copy for information to:

Data Protection Officer

How to appeal

If you want to appeal the decision, you must write to the Data Inspectorate. Enter i

the letter which decision you are appealing and the change you are requesting.

The appeal must have been received by the Data Inspectorate no later than three weeks from

the day the decision was announced. If the appeal has been received in due time

The Data Inspectorate forwards it to the Administrative Court in Stockholm

examination.

You can e-mail the appeal to the Data Inspectorate if it does not contain

any privacy-sensitive personal data or data that may be covered by

secrecy. The authority's contact information can be found on the first page of the decision.