Decision

Diarienr

2020-12-02

DI-2019-3839

Ert diarienr

The board of Karolinska

University Hospital

Karolinska University Hospital Solna

171 76 Stockholm

Supervision under the Data Protection Regulation -

needs and risk analysis and access issues

in journal system

Content

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

The Data Inspectorate's decision

The Data Inspectorate has during an inspection on March 27, 2019 found that

The board of Karolinska University Hospital (Karolinska

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.

Karolinska 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 take place in the journal system TakeCare, in accordance with ch. 2

§ and ch. 6 Section 7 of the Patient Data Act (2008: 355) and Chapter 4 § 2

The National Board of Health and Welfare's regulations and general guidelines (HSLF-FS 2016: 40) on record keeping and processing of personal data in health and healthcare. This means that Karolinska University Hospital does not have taken appropriate organizational measures to be able to ensure and be able to show that the processing of personal data has a security that is appropriate in relation to the risks.

Karolinska University Hospital has not limited users' permissions for accessing the journal system TakeCare 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 HSLF-FS 2016: 40. This means that Karolinska The University Hospital has not taken measures to be able to ensure and be able to demonstrate appropriate security for personal data.

The Data Inspectorate decides on the basis of Articles 58 (2) and 83 i the Data Protection Ordinance and Chapter 6 § 2 of the law (2018: 218) with additional provisions to the EU Data Protection Regulation that Karolinska University Hospital, for violation of Article 5 (1) (f) and (2) 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).

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

administrative sanction fee of SEK 4,000,000 (four million).

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

data protection ordinance Karolinska University Hospital to ensure that

required needs and risk analysis is performed and documented for

the journal system TakeCare and that thereafter, with the support of needs and

risk analysis, each user is assigned individual privileges to access

personal data to only what is needed for the individual to be able to

perform their duties in health care, in accordance with

Article 5 (1) (f) and Article 32 (1) and (2) of the Data Protection Ordinance, Chapter 4 § 2 and

Chapter 6 Section 7 of the Patient Data Act and Chapter 4 2 § 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 March 27, 2019 reviewed Karolinska University Hospital

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

risk analysis. The review has also included how Karolinska

The University Hospital assigned privileges for access to

the main journal system TakeCare, and what access options they assigned

the authorizations provide within both the framework of the internal secrecy according to ch.

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

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

documentation of access (logs) that is in the record system.

The Data Inspectorate has only examined users' access possibilities to

the medical record system, ie what care documentation the user actually has

can take part in and read. The review does not include which features

is included in the authorization, ie what the user can actually do in

the journal system (for example, issuing prescriptions, writing referrals, etc.).

Previous review of Karolinska University Hospital's eligibility management

The Data Inspectorate has previously carried out an inspection regarding Karolinska

The University Hospital's eligibility management, etc. By the Data Inspectorate

decision with registration number 920-2012, announced on 26 August 2013, appears

that Karolinska University Hospital i.a. was instructed to carry out a needs and risk analysis as a basis for allocating

authorizations in TakeCare. With

Due to the decision, Karolinska University Hospital submitted one

written answer on 18 December 2013. The answer states, among other things. to Karolinska

The University Hospital had begun work on developing an action plan

and a needs and risk analysis.

What has emerged in the case

Karolinska University Hospital has mainly stated the following.

Personal data manager

Karolinska University Hospital is a separate authority within the Region

Stockholm. The board of Karolinska University Hospital is

personal data controller for the processing of personal data that

Karolinska University Hospital performs in the main medical record system TakeCare.

Organisation

The care at Karolinska University Hospital is organized from the outside

medical thematic areas and a number of functions that bring together competencies.

Wards, receptions and day care are organized according to themes.

Each theme is divided into a number of patient areas, which gather similarities

patient flows. Function is an area of competence that runs across

teman. A function assists with skills and resources, which are used in

many different patient groups and thus in several themes. There is a

patient area manager and a function area manager for each area.

Journal system

Karolinska University Hospital uses TakeCare as

main journal system, and participates in TakeCare's cohesive system

record keeping.

Karolinska University Hospital manages TakeCare, and has

signed the agreement with the supplier. Karolinska University Hospital has

thus a large number of personal data assistant and sub-assistant agreements with

other care providers.

There is both a regional and a local organization for TakeCare. The

the regional organization consists of a management group (steering group), which

in addition to Karolinska University Hospital consists of representatives of six

other care providers.

Users and patients

Karolinska University Hospital has almost 16,000 employees in total. The number

users in the TakeCare journal system who are employed by Karolinska

The University Hospital has 12,285 members, of which 1,328 are users

inactive. At the time of the inspection, there were thus 10,957 active users.

A user account is automatically deactivated if no login has taken place on 60

days.

The TakeCare medical record system contains medical records for approximately 3 million patients.

Of these, 1,970,000 patient records are registered on, and de facto patients

at, Karolinska University Hospital.

The cohesive record keeping in TakeCare comprises approximately 200-400

healthcare providers. It is today possible to search for all social security numbers available

and TakeCare. However, there are discussions regionally about limiting in some cases

the ability to search for information to a limited number of patients, to

example patients in a particular accommodation.

Internal secrecy

Needs and risk analysis

Karolinska University Hospital can not submit with any performed

needs and risk analysis for TakeCare. It is the respective patient area and

functional area manager who will implement and document needs and

risk analyzes before granting authorizations. However, it is investigated regularly

what needs there are and what competencies employees should be assigned,

for example in new hires. The template for needs and risk analyzes that

are in Karolinska University Hospital's guidelines are not met

regularly.

Karolinska University Hospital can not answer about the work that began

following the Data Inspectorate's previous supervisory decision of 26 August 2013

resulted in a needs and risk analysis for TakeCare.

After the inspection, Karolinska University Hospital has begun work

to ensure that needs and risk analyzes are carried out throughout

the organization. Among other things, a needs and risk analysis has been carried out for

the function Perioperative Medicine and Intensive Care in accordance with Karolinska

The University Hospital's guidelines.

Authorization of access to personal data about patients

There are about 40 authorization profiles in TakeCare that contain features

such as "reading recipes". Of these, 26 are so-called reading functions. There are, among other things, two eligibility profiles

for nurses,

where what distinguishes the profiles is that one has automated login.

This means that login takes place automatically at the care unit you belong to

one authorization profile, but not for the other. Also for doctors available

there are two authorization profiles. What distinguishes the profiles is that one has

access to a so-called emergency room. As a user, you can have several different ones

eligibility profiles, but not exceeding five. For example, a drug candidate may have

have been assigned permissions from several different devices. The staff bends in

such cases themselves in the journal filter in TakeCare, which means that they do one

active choice to take part in the patient's information on different devices. About one

users tick the option "all devices" so no further active is needed

choice to access patient information from all devices. Even if it

If there are different authorization profiles, Karolinska states that the users “have

access to all patients in TakeCare ”.

All accounts are individual, ie there is no account like several

users can use (group account).

In the governing document "Decision on allocation of eligibility" from 2015 (latest updated 23 October 2018) 2 a general description of the regulations is given and the conditions for assigning authorizations. It also contains one description of an approach to conducting a needs and risk analysis, based on the user's need to have access to personal data about patients in their work and refers to the allocation of eligibility profile. In the guideline further reminds of certain relevant issues. It is also stated that some of the examples do not match the eligibility profiles available.

After the inspection, Karolinska University Hospital performed a needs and risk analysis for the function Perioperative Medicine and Intensive Care. In this states that the risks to be considered are those that arise if employees within the business do not have access to relevant information, as well as risks related to too broad or generous access to patient information.

The guideline "Allocation of authorizations" has been developed by lawyers and established by the chief physician in the field of quality and patient safety.

2

Access to the Stockholm County healthcare area's personal data about patients

During the inspection, it emerged that users at Karolinska The University Hospital has access to information about patients within Stockholm County Healthcare Area (SLSO). According to Karolinska The University Hospital is due to the fact that Karolinska University Hospital

and SLSO are listed as "one and the same" care unit in TakeCare. This means that users at Karolinska University Hospital technically have access also to data on patients at SLSO in the field of internal confidentiality, and vice versa.

As for the background and motives for Karolinska University Hospital and SLSO is listed as a care unit in TakeCare, Karolinska has The University Hospital referred to an enforcement decision dated 2010-01 and a minutes of board meetings. The minutes state that The county council director in the enforcement decision has stated that Stockholm läns landstings (SLL) administrations that provide health and medical care belong to the care provider SLL and that this means that Karolinska University Hospital and SLSO, for the time being, shall remain unchanged as one and the same care providers in TakeCare.

Coherent record keeping

Needs and risk analysis

No needs and risk analysis has been performed before the staff has granted access to other care providers' care documentation within the framework of coherent record keeping.

Authorization of access to personal data about patients

Users at Karolinska University Hospital have access to others caregivers' data on patients in TakeCare within the framework of coherent record keeping. Access is prepared based on the patient, and requires patient consent. When searching for a patient, the caregivers are shown as the patient previously sought care from. This gives an indication that it can is information about the patient at another healthcare provider. The information can be important in, for example, prescribing drugs. By doing one

active selection and clicking on a specific device can be accessed

the information.

There is a decision from the Stockholm Region that every care provider chooses

to use the journal system TakeCare must also be included in

coherent record keeping.

Karolinska University Hospital has a governing document “Access to

patient record, guideline ”, which applies from 17 August 20183. The guideline

contains a general description of the regulations and states them

the conditions for taking part in the care documentation in TakeCare in some

situations.

Technical restrictions in TakeCare regarding access to

personal data about patients

The technical limitations regarding users' accessibility such as

used by Karolinska University Hospital concerns so-called protected units

and TakeCare. There are currently six such devices, among others

ANNOVA, the SESAM reception and the child protection team.

With regard to the protected care units, it is not possible to limit

competencies at the individual level, but on the other hand, access to

medical records regarding these patients are limited to a defined one

user group. The protected units are not visible when held together

record keeping and they are also not included in the standard profile role in the record filter.

Decisions on protected units have been preceded by an assessment based on both

a patient safety and an integrity perspective. Protected care units

is used today only to a limited extent. This because one more

extensive use would pose significant patient safety risks.

Karolinska University Hospital has stated in a supplementary statement

following.

Technical restrictions regarding the access of individual executives:

The electronic record system TakeCare enables restriction of access by each

care unit can control what information each user group (usually occupational group)

at the device can see and what each user group can do. The care unit can continue

control what information other user groups at other care units can see respectively

do. As TakeCare is configured today, however, only control is enabled

The guideline "access to patient records, guideline" has been developed by lawyers and established by

the chief physician in the field of quality and patient safety.

user group level. Any possibility of technical limitation for individual executives

access possibilities do not exist. This applies both within the so-called internal secrecy as within

the framework for access through coherent record keeping. Regarding the hospital's so-called protected

care units, it is also not possible to limit qualifications at the individual level, but it is possible

access to medical records regarding these patients is limited to a defined one

user group.

The possibility for a care provider to opt out of access to the other care providers

patient documentation in TakeCare

Following a decision from the Stockholm Region, every care provider who chooses to use it must

The TakeCare record system is also part of cohesive record keeping. This means that a

caregivers cannot restrict other caregivers' access to their own care documentation.

The individual care provider, on the other hand, can control its users' access to information in it

coherent record keeping. The TakeCare journal system offers features that provide

the ability of the caregiver to limit the competence of its users in such a way that they only

has access to journal entries from, for example, a specially specified group with others

healthcare providers. To illustrate this, Karolinska University has referred to a screenshot,

which shows eligibility per care provider.

From the screenshot it can be read that it is possible to control at unit level

the competence of a unit's users in relation to other care providers

devices by setting them to "see document" - or "do not see"

documents ”lists. The latter list shows that it is possible to block

units at other care providers. However, it does not appear that the function exists per

caregiver, without having to block all units of the caregiver in question

if you want to block a care provider.

Documentation of access (logs)

Karolinska University Hospital has displayed various logs and stated in

essentially the following.

There are two different types of logs, in-depth logs and targeted logs.

In-depth log information can be requested on either user

(the employee) or on the patient. A targeted log information can be requested by

for example, a patient.

A screenshot showing the documentation in the logs shows the following

information is registered in the log; patient, status, time, user, system,

performed server calls (action) and from which care unit the action was performed.

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 the person responsible for personal data must be responsible for and be able to show that they the basic principles of 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, provided that at least one of the conditions of Article 6 (1) is 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 provisions 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 as to 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 the internal secrecy, that is

say regulates how the privacy protection is to be handled within a care provider

activities and especially 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.

Of ch. 4 § 2 HSLF-FS 2016: 40 follows that 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

Provisions in Chapter 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 also applies

for authorization allocation for unified record keeping. The requirement 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. the documentation of the access (logs) states 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 Karolinska 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 security of the treatment is regulated more specifically in Article 5 (1) (f)

and Article 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 also 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 against actors outside 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

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 patient data.

Both the needs and the risks must be assessed on the basis of the information provided

need to be addressed in the business, what processes it is a matter of 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.

When the Data Inspectorate has requested a needs and risk analysis

Karolinska University Hospital referred to the governing document “Decision on

eligibility allocation, guideline ”4 (eligibility allocation guidelines) and

stated that it is the respective patient area and function area manager

who must carry out and document needs and risk analyzes before

allocation of authorizations. According to Karolinska University Hospital, this is done

when allocating qualifications, for example for new hires, on a regular basis

an investigation of what the employee's need for competence also is

the template for needs and risk analyzes contained in the guideline is not filled in

regularly. Karolinska University Hospital was able at the time of

the inspection does not present a needs and risk analysis performed, but has

afterwards stated that they had begun work to ensure that the needs and

risk analyzes are performed in the business. They have also submitted a documented

"Needs and risk analysis" for the functional area Perioperative Medicine.

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

4

"Decision on authorization allocation, guideline" which applies from 23 October 2018.

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 activities. It should

suitably result in authorization assignments but it is

not the instructions to the person assigning permissions that are the analysis.

At the time of the inspection, Karolinska University Hospital was unable to

present a needs and risk analysis. The latter submitted needs and
the risk analysis regarding the function Perioperative Medicine does not meet
the data protection provisions' requirements for such an analysis according to ch. § 2 HSLFFS 2016: 40, as it constitutes a
general description of work tasks in
TakeCare for some specific occupational categories. The document contains none
analysis of what tasks employees need to be able to perform their
tasks. The document does not contain an analysis of the risks that may
be associated with an too at availability regarding various types of
personal data.
The Data Inspectorate further states that the approach described in
eligibility guidelines to analyze which eligibility
to be assigned to an individual user based on the existing ones
the eligibility profiles. These are created based on what users need
be able to do with the tasks, such as reading or writing, and not from the outside
what information about the patient the individual user needs to have
access to be able to perform their work.
The needs and risk analyzes described in Karolinska University Hospital's
eligibility guidelines are not an analysis according to the requirements of a
needs and risk analysis in accordance with the data protection regulations. Karolinska
The University Hospital has also not been able to show that the work that was started
after the previous review in 2013 resulted in the implementation of a
needs and risk analysis for TakeCare in accordance with the injunction.
The Data Inspectorate can thus state that Karolinska
The University Hospital's allocation of qualifications has not been preceded by one
necessary needs and risk analysis.
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, including that there should be different

authorization categories in the medical record system and that the authorizations shall

limited to what the user needs to give the patient a good and safe

care. It also appears that “a more extensive or coarse-meshed

allocation of competences should be considered as an unjustified dissemination of

journal information within an activity and as such should not be 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.
In addition to Karolinska University Hospital's guideline for awarding
permissions, there is also a control document “Access to patient records,
guideline ”(guidelines on access), valid from 17 August 2018.5
However, the guidelines only provide a general description of the regulations and
describes the conditions for the allocation of authorizations and for
to take part in the care documentation in TakeCare in different situations.
The Data Inspectorate notes that even if each user de facto has
has been granted an individual authorization, the assigned authorizations have not
The guideline "access to patient records, guideline" is established by the chief physician in the area
quality and patient safety, and lawyers have participated in the development area.
5

limited in a way that ensures that the user does not have
access to more personal data about patients or personal data
if more patients than he needs to perform his work. They assigned
the permissions instead mean that the user has access to basically everyone
personal data about patients in TakeCare. This is because there are only two
eligibility profiles for nurses and doctors respectively, and where the only one

that distinguishes the eligibility profiles is that one
the nurse's authorization has an automated login to that care unit
the staff belongs to and one of the doctors has access to a so-called
emergency room. The restriction that has otherwise emerged regarding
access possibilities to personal data in the record system refers to so-called
protected devices.

Against this background, the Data Inspectorate considers that, since the allocation
of qualifications not preceded by a necessary needs and risk analysis, no
there were conditions to limit assigned privileges or there was support
to determine what are justified access opportunities for executives
at Karolinska University Hospital.

That the allocation of authorizations has not been preceded by a need and
risk analysis means that Karolinska 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 options
which are justified to users on the basis of such an analysis. Karolinska
The University Hospital has thus not taken appropriate organizational measures
measures, in accordance with Article 32 of the Data Protection Regulation, to limit
users' access to personal data about patients in the medical record 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. The number
users at Karolinska University Hospital are close to 11,000 and
TakeCare contains personal data concerning approximately 3 million patients, of which
about 2 million have been patients at Karolinska University Hospital.

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

Karolinska 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:

Karolinska University Hospital has not restricted users

permissions for accessing the TakeCare 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 Karolinska University Hospital

have not taken measures to ensure and, in accordance with Article

5.2 Data Protection Regulation, be able to demonstrate appropriate security for

personal data.

Documentation of access in logs

The Data Inspectorate states that it appears from the logs in TakeCare

information about the specific patient, which user has opened

the journal, measures that have been taken, which journal entry has

opened, what time period the user has been in, all openings of

the record made on that patient during the selected time period and

time and date of last opening. According to the Data Inspectorate

assessment, this is in accordance with the requirements for documentation of

accesses in the logs set out in the National Board of Health and Welfare's regulations.

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 instead 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) sets out the factors to be taken into account in determining whether a

administrative penalty fee shall be imposed, but also what shall affect

the size of the penalty fee. Of central importance for the assessment of

the seriousness of the infringement is its nature, severity and duration. If

in the case of a minor infringement, the supervisory authority may, according to reasons

148 of the Data Protection Regulation, issue a reprimand instead of imposing one

penalty fee.

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 size of the data collections and how many
sharing information with each other has increased significantly. This increases the demands on
the personal data controller, as the assessment of what is an appropriate
safety is affected by the extent of the treatment.
In health care, this means even greater responsibility for it
personal data controller to protect the data from unauthorized access,
among other things by having an authorization allocation that is atomized. The
It is therefore essential that there is a real analysis of the needs based on different
businesses and various executives. Equally important is that it happens one
actual analysis of the risks that may arise from an integrity perspective
in the event of an excessive allocation of access rights. Based on this analysis
shall then restrict the access of the individual executive. This
eligibility must then be followed up and changed or gradually reduced
as changes in the tasks of the individual executive result
reason for it.
The Data Inspectorate's inspection has shown that Karolinska University Hospital does not
has taken appropriate security measures to provide protection to
the personal data in the record system by Karolinska
The university hospital in its capacity as personal 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. Karolinska
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, with the support of 58.2 d i

the Data Protection Ordinance, Karolinska University Hospital to ensure that

The required needs and risk analysis for the TakeCare medical record system is carried out

within the framework of both internal confidentiality and within it

coherent record keeping. The needs and risk analysis must be documented.

Karolinska University Hospital will continue, with the support of needs and

risk analysis, assign each user individual privileges to access

personal data that is limited to only what is needed for it

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

Penalty fee

The Data Inspectorate can state that the violations are fundamentally related

Karolinska 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 very large data collections 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

patient information in the main medical record system belongs to the core of a healthcare provider

activities, that the treatment includes many patients and the possibility of

access refers to a large proportion of employees. In this case, it's about

about 2,000,000 patients in the field of internal confidentiality and

about another 1,000,000 patients within the cohesive framework

record keeping. There are only six so-called protected units there

the data is not accessible to users outside these devices.

The Data Inspectorate can also state that Karolinska

The University Hospital did not follow the Data Inspectorate's previous injunction from

on 26 August 2013 to carry out a needs and risk analysis which

basis for allocation of authorizations in accordance with the then requirement in ch. 6

§ second paragraph second sentence SOSFS 2008: 14, which corresponds to the current one

provision in ch. 4 2 § HSLF-FS 2016: 40. This is an aggravating circumstance

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 Karolinska

The university hospital for several years, which means that the action took place intentionally and thus is considered more serious.

In determining the seriousness of the infringements, it can also be stated that the infringements also cover the basic principles set out in Article 5 (i) the Data Protection Regulation, which belongs to the categories of more serious infringements which may give rise to a higher penalty under Article 83 (5) (i) the Data Protection Regulation.

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 these 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 these infringements.

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

Karolinska University Hospital to SEK 4,000,000 (four million).

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 also handled by the General Counsel Hans-Olof Lindblom, the unit managers

Katarina Tullstedt and Malin Blixt, as well as the lawyer Maja Savic participated.

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

Appendix:

How to pay 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

on 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.

2 8 (28)