Decision

Diary no

2020-12-02

DI-2019-3839

Your diary no

The board of Karolinska

University Hospital

Karolinska University Hospital Solna

171 76 Stockholm

Supervision according to the Data Protection Regulation –

needs and risk analysis and issues of access

in journal systems

Content

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

The Swedish Data Protection Authority's decision

The Swedish Data Protection Authority has, during an examination 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 as well as article 32.1 0ch 32.2 of the data protection regulation1 by

1.

Karolinska University Hospital in capacity of

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

carried out a needs and risk analysis before awarding of

authorizations take place in the record system TakeCare, in accordance with ch. 4 2 § and ch. 6 Section 7 of the Patient Data Act (2008:355) and Chapter 4. Section 2

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

record keeping and processing of personal data in health and

healthcare. This means that Karolinska University Hospital does not

has taken appropriate organizational measures to be able to

ensure and be able to demonstrate that the processing of the personal data has

a security that is suitable in relation to the risks.

2. Karolinska University Hospital has not limited

the users' authorizations for access to the records system

TakeCare to what is only necessary 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 ch. 4 Section 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

the personal data.

Datainspektionen decides with the support of articles 58.2 and 83 i

the data protection regulation and ch. 6 Section 2 of the Act (2018:218) with

supplementary provisions to the EU data protection regulation that

Karolinska University Hospital, for violation of article 5.1 f and 5.2

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

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

of such data and on the repeal of Directive 95/46/EC (general

data protection regulation).

1

as well as article 32.1 and 32.2 of the data protection regulation must pay a

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

Datainspektionen orders with the support of article 58.2 d i

data protection regulation Karolinska University Hospital to ensure that

required needs and risk analysis is carried out and documented for

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

the risk analysis, each user is assigned individual authorization for access to

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

fulfill their duties in health care, in accordance with

article 5.1 f and article 32.1 and 32.2 of the data protection regulation, ch. 4 § 2 and

6 ch. Section 7 of the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40.

Account of the supervisory matter

The Swedish Data Protection Authority started supervision by letter on 22 March 2019 and has

on site on March 27, 2019 reviewed about Karolinska University Hospital

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

risk analysis. The review has also covered how Karolinska

University Hospital assigned permissions for access to

the TakeCare master record system, and what access opportunities they assigned

the authorizations provide both within the framework of the internal secrecy according to ch. 4.

the patient data act, such as the integrated record keeping according to ch. 6

the patient data act. In addition to this, the Swedish Data Protection Authority has also reviewed which

documentation of access (logs) contained in the records system.

The Swedish Data Protection Authority has only reviewed users' access options

the record system, i.e. which care documentation the user actually uses

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

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

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

Previous review of Karolinska University Hospital's authorization management

The Swedish Data Protection Authority has previously carried out an inspection regarding Karolinska

The university hospital's authorization control, etc. By the Data Inspectorate

decision with diary number 920-2012, announced on 26 August 2013, states

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

authorizations in TakeCare. With

reason for the decision, Karolinska University Hospital received a

written answer on 18 December 2013. The answer shows, among other things, that Karolinska

The university hospital had begun work on developing an action plan

and a needs and risk analysis.

What emerged in the case

Karolinska University Hospital has essentially stated the following.

Personal data controller

Karolinska University Hospital constitutes its own authority within the Region

Stockholm. It is the board of the Karolinska University Hospital

personal data controller for the processing of personal data that

Karolinska University Hospital performs TakeCare in the main record system.

Organisation

Care at Karolinska University Hospital is organized externally

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

Care wards, receptions and day care are organized according to themes.

Each theme is divided into a number of patient areas, which bring together similar ones

patient flows. Function is an area of expertise that runs right through

themes. 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 functional area manager for each area.

Journal system

Karolinska University Hospital uses TakeCare as

main record system, and participates in TakeCare's system for cohesion

record keeping.

Karolinska University Hospital manages TakeCare, and has

signed the contract with the supplier. Karolinska University Hospital has

thus a large number of personal data processor and subprocessor agreements with

other healthcare providers.

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

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

apart from Karolinska University Hospital consists of representatives for sex

other healthcare providers.

Users and patients

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

users of the TakeCare record system who are employed at Karolinska

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

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

A user account is automatically deactivated if no login has occurred in 60

days.

The TakeCare record system contains 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 integrated record keeping in TakeCare includes approx. 200-400

healthcare providers. Today, it is possible to search all social security numbers that exist

in TakeCare. There are, however, regional discussions about restricting in some cases

the possibility of seeking information for a limited number of patients, to

for example, patients in a certain accommodation.

Internal confidentiality

Needs and risk analysis

Karolinska University Hospital cannot submit any performed

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

functional area manager who must carry out and document needs and

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

which needs exist and which authorizations should be assigned to employees,

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

are in Karolinska University Hospital's guidelines, however, they are not filled out

regularly.

Karolinska University Hospital cannot answer about the work that was started

following Datainspektionen's previous supervisory decision from 26 August 2013

resulted in a need and risk analysis for TakeCare.

After the inspection, Karolinska University Hospital has started 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 Perioperative Medicine and Intensive Care function in accordance with Karolinska

The University Hospital's guidelines.

Authorization assignment regarding access to personal data about patients

There are about 40 authorization profiles in TakeCare that contain functions

such as "read recipe". Of these, 26 are so-called reading functions. There are, among other things, two qualification profiles for

nurses,

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

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

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

there two authorization profiles. What differentiates the profiles is that one has

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

authorization profiles, but no more than five. For example, a medical candidate may have

been assigned permissions from several different entities. The staff check in

such cases themselves in the record filter in TakeCare, which means they make a

active choice to access the patient's information on different devices. About one

user ticks the "all devices" option, nothing further active is needed

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

are different authorization profiles, then Karolinska states that users "have

access to all patients in TakeCare".

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

users can use (group account).

In the governing document "Decision on authorization allocation" from 2015 (latest

updated on 23 October 2018)2 a general description of the regulations is given

and the prerequisites for assigning permissions. It also contains a

description of an approach to carry out a needs and risk analysis,

which is based on the user's need to have access to personal data about

patients in their work and refers to the assignment of an authorization profile. In the guideline

is further reminded of certain relevant issues. It is also stated that some

of the examples do not match the authorization profiles available.

After the inspection, Karolinska University Hospital carried out a needs and

risk analysis for the Perioperative Medicine and Intensive Care function. In this

states that the risks to be taken into account 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 "Assignment of authorizations" was developed by lawyers and established by

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

2

Access to Stockholm County's health care area's personal data on patients

The inspection revealed that users at Karolinska

The university hospital has access to information about patients within

Stockholm county health care area (SLSO). According to Karolinska

University Hospital This is because 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 information about patients at SLSO within the internal secrecy, and vice versa.

Regarding the background and motives for Karolinska University Hospital and SLSO is listed as a care unit in TakeCare, Karolinska has University Hospital referred to an enforcement decision dated 2010-01 and a board meeting minutes. It appears from the protocol that the county council director in the enforcement decision has stated that Stockholm's county council (SLL) administrations that provide health care belong to the healthcare provider SLL and that this means that Karolinska University Hospital and SLSO, for the time being, shall remain unchanged as one and the same caregivers in TakeCare.

Coherent record keeping

Needs and risk analysis

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

Authorization assignment regarding access to personal data about patients

Users at Karolinska University Hospital have access to others care provider's information about patients in TakeCare within the framework of coherent record keeping. Access is prepared based on patient, and requires patient consent. When searching for a patient, the healthcare providers who the patient previously sought care from. This gives an indication that it can there is information about the patient with another healthcare provider. The information can be important when, for example, prescribing medicine. By making one

active selection and clicking into a particular device can be accessed

the information.

There is a decision from Region Stockholm that every healthcare provider who chooses

using the TakeCare record system must also be included

coherent record keeping.

Karolinska University Hospital has a steering document "Access to

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

contains a general description of the regulatory framework and it states

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

situations.

Technical limitations in TakeCare regarding access to

personal data about patients

The technical limitations regarding user access that

used by Karolinska University Hospital for so-called protected units

in TakeCare. There are currently six such units, among others

ANNOVA, the SESAM reception and the child protection team.

As far as the protected care units are concerned, it is not possible to restrict

permissions at the individual level, but in contrast, access to

medical record documentation regarding these patients is limited to a defined

user group. The protected devices are not visible when joined

journaling and they are also not included in the default profile role in the journal filter.

The decisions about protected units have been preceded by an assessment from the outside as well

a patient safety and 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 individual executives' access:

The TakeCare electronic medical record system enables restriction of access by each

care unit can control which information the respective user group (usually professional group)

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

control which 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" was drawn up by lawyers and established by

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

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

access possibilities are not available. This applies both within the so-called the inner 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 authorizations on an individual level, but on the other hand it is possible

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

user group.

The possibility for a caregiver to opt out of the access of the other caregivers

patient documentation in TakeCare

Following a decision from the Stockholm Region, every healthcare provider who chooses to make use of the TakeCare record system also be included in coherent record keeping. This means that a care providers cannot restrict other care providers' access to their own care documentation.

The individual healthcare provider, however, can control their users' access to information in it coherent record keeping. The TakeCare journal system offers functions that provide the healthcare provider has the opportunity to limit their users' authorization in such a way that they only have 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 healthcare provider.

It can be deduced from the screenshot that it can be controlled at the unit level the authority of a device's user in relation to that of other healthcare providers devices by setting them to “see document” or “not see documents” lists. From the latter list it appears that it is possible to block units with other healthcare providers. However, it does not appear that the function exists per care provider, but you must block all devices of the current care provider if you want to block a care provider.

Documentation of the access (logs)

Karolinska University Hospital has shown various logs and stated in mainly the following.

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

From a screenshot, which shows the documentation in logs, it appears that the following data is recorded in the log; patient, status, time, user, system, performed server call (action) and from which care unit the action was performed.

Justification of the decision

Applicable rules

The Data Protection Regulation the primary legal source

The Data Protection Regulation, often abbreviated GDPR, was introduced on May 25, 2018 and is the primary legal regulation when processing personal data. This also applies in healthcare.

The basic principles for processing personal data are stated in Article 5 of the Data Protection Regulation. A basic principle is the requirement of security according to Article 5.1 f, which states that the personal data must be processed in a way that ensures appropriate security for the personal data, including protection against unauthorized or unauthorized processing and against loss, destruction or damage by accident, using appropriate technical or organizational measures.

Article 5.2 shows the so-called liability, that is to say that the personal data controller must be responsible for and be able to demonstrate that they the basic principles in paragraph 1 are complied with.

Article 24 deals with the responsibility of the personal data controller. Of Article 24.1 it appears that the person in charge of personal data is responsible for carrying out appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with the data protection regulation. The actions shall carried out taking into account the nature, scope and context of the treatment and purpose as well as the risks, of varying degree of probability and seriousness, for

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

if necessary.

Article 32 regulates security in connection with processing. According to point 1

must the personal data controller and the personal data assistant with consideration

of the latest developments, implementation costs and treatment

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

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

take appropriate technical and organizational measures to ensure a

security level that is appropriate in relation to the risk (…). According to point 2 shall

when assessing the appropriate security level special consideration is given to the risks

which the processing 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 when assessing the risk of natural persons

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

personal data subject to confidentiality, information about health or

sexual life, if there is processing of personal data concerning vulnerable physical

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

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

Furthermore, it follows from reason 76 that how probable and serious the risk for it

Data subjects' rights and freedoms should be determined based on the processing

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

basis of an objective assessment, through which it is determined whether

the data processing involves a risk or a high risk.

Recitals 39 and 83 also contain writings that provide guidance on it

closer to the meaning of the data protection regulation's requirements for security at

Processing of personal data.

The Data Protection Regulation and the relationship with supplementary national

regulations

According to Article 5.1 a of the data protection regulation, the personal data must

processed in a legal manner. In order for the treatment to be considered legal, it is required

legal basis, in that at least one of the conditions in Article 6.1 is met.

Provision of health care is one such task of generality

interest referred to in Article 6.1 e.

In healthcare, the legal bases can also be legal

obligation in Article 6.1 c and exercise of authority according to Article 6.1 e

updated.

When it comes to the question of the legal bases legal obligation, generally

interest and the exercise of authority are given to the Member States, according to Article

6.2, retain or introduce more specific provisions to adapt

the application of the provisions of the Regulation to national conditions.

National law can further determine specific requirements for data processing

and other measures to ensure legal and fair treatment. But

there is not only a possibility to introduce national rules but also a

duty; Article 6.3 states that the basis for the processing 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 special provisions to adapt the application of the provisions of data protection regulation. Union law or Member States' national law right must fulfill an objective of public interest and be proportionate to it legitimate goals pursued.

Article 9 states that treatment of special categories of personal data (so-called sensitive personal data) is prohibited. Sensitive personal data includes, among other things, information about health. Article 9.2 states the exceptions where sensitive personal data may still be processed.

Article 9.2 h states that processing of sensitive personal data may take place if the processing is necessary for reasons related to, among other things provision of healthcare on the basis of Union law or Member States' national law or according to agreements with professionals on health area and provided that the conditions and safeguards which referred to in point 3 are met. Article 9.3 requires regulated confidentiality.

This means that both the legal bases public interest, exercise of authority and legal obligation such as treatment of sensitive personal data with the support of the exception in Article 9.2 h needs supplementary rules.

Supplementary national regulations

For Swedish purposes, both the basis for the treatment and the the special conditions for processing personal data within health and healthcare regulated in the Patient Data Act (2008:355), and the patient data regulation (2008:360). In ch. 1 Section 4 of the Patient Data Act states that

the law supplements the data protection regulation.

The purpose of the Patient Data Act is that information management within health and

healthcare must be organized so that it caters for patient safety and

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

personal data must 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 gain access

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

According to ch. 2 Section 6 of the Patient Data Act is a healthcare provider responsible for personal data

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

and a municipality is any authority that provides health 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 legislature has

thus, through the regulation, a balance has been made in terms of how

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

such as the right to personal integrity when processing personal data.

The National Board of Health and Welfare has issued regulations with the support of the patient data regulation

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

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

supplementary rules, which must be applied when healthcare providers treat

personal data in healthcare.

National regulations that supplement the data protection regulation's requirements for security can be found in chapters 4 and 6. the Patient Data Act and chs. 3 and 4 HSLF-FS 2016:40.

Requirements to carry out needs and risk analysis

The care provider must according to ch. 4. § 2 HSLF-FS 2016:40 make a need-and risk analysis, before assigning authorizations in the system takes place.

That an analysis of the needs as well as the risks is required is evident from the preparatory work to the Patient Data Act, prop. 2007/08:126 pp. 148-149, as follows.

Authorization for the staff's electronic access to information about patients must be limited to what the executive needs to be able to perform his duties in health and healthcare. It includes, among other things, that authorizations must be followed up and changed or restricted accordingly hand as changes in the individual executive's duties give rise to it.

The provision corresponds in principle to Section 8 of the Care Register Act. The purpose of the provision is to inculcate the duty of the responsible health care provider to make active and individual authorization assignments based on analyzes of which detailed information different personnel categories and different types of operations need. But it is not only necessary needs analyses. Risk analyzes must also be carried out where different types of risks are taken into account such as may be associated with excessively wide availability regarding certain types of information.

Protected personal data marked confidential, information about publicly known persons,

data from certain clinics or medical specialties are examples of categories such as may require special risk assessments.

Generally speaking, it can be said that the more extensive an information system is, the greater the quantity different authorization levels there must be. Decisive for decisions on eligibility for e.g. various categories of healthcare professionals to electronic access to records i patient records should be that the authorization should be limited to what the executive needs for the purpose of good and safe patient care. A more extensive or coarse meshed assignment of authorization should - even if it would have points from an efficiency point of view - be considered as an unjustified dissemination of medical records within a business and as such should not accepted.

Furthermore, data should be stored in different layers so that more sensitive data requires active choices or otherwise are not as easily accessible to staff as less sensitive information. When it applies to personnel who work with operational follow-up, statistical production, central financial administration and similar activities that are not individual-oriented, probably the majority of executives have access to information that can only be derived indirectly to individual patients. Electronic access to code keys, social security numbers and others information that directly points out individual patients should be able to be strong in this area limited to single persons.

Internal confidentiality

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

It appears from ch. 4. Section 2 of the Patient Data Act that the healthcare provider must decide conditions for granting authorization to access such information about patients who are transported fully or partially automated. Such authorization shall is limited to what is needed for the individual to be able to fulfill their duties

tasks within health care.

Of ch. 4 § 2 HSLF-FS 2016:40 follows that the care provider must be responsible for each

users are assigned an individual authorization for access to

personal data. The healthcare provider's decision on the allocation of authorization shall

preceded by a needs and risk analysis.

Coherent record keeping

Provisions in ch. 6 the Patient Data Act concerns coherent record keeping,

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

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

care provider for purposes related to care documentation. Access to

information occurs through a healthcare provider making the information about a patient

which the healthcare provider registers about the patient available to other healthcare providers

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

Of ch. 6 Section 7 of the Patient Data Act follows that the regulations in ch. 4 also applies

for authorization assignment in case of joint record keeping. The requirement to

the care provider must carry out a needs and risk analysis before awarding

authorizations in the system takes 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 healthcare provider must ensure that

access to such patient data that is held in whole or in part

automatically documented and systematically checked.

According to ch. 4 § 9 HSLF-FS 2016:40 the care provider must be responsible for

1. it is clear from the documentation of the access (logs) which

actions taken with data about a patient;

2. the logs show which care unit or care process

the measures have been taken,

3. it is clear from the logs at which time the measures were taken,

4. the identity of the user and the patient can be seen from the logs.

The Swedish Data Protection Authority's assessment

Personal data controller's responsibility for security

As described above, in the National Board of Health and Welfare's regulations, the care provider is given a

responsibility for information management in healthcare, such as, for example,

conduct a needs and risk analysis before granting authorizations i

the system takes place. In the public health and medical care does not coincide

always the concept of care provider with the personal data controller.

Of both the basic principles in Article 5 and Article 24.1

data protection regulation, it appears that it is the personal data controller

which must implement appropriate technical and organizational measures to

ensure and be able to demonstrate that the treatment is carried out in accordance with

data protection regulation.

The Data Protection Authority can state that the data protection regulation in the capacity of

The EU regulation is directly applicable in Swedish law and that in the regulation

is specified when supplementary regulation must or may be introduced nationally. There is

for example space to nationally regulate who is

personal data controller according to Article 4 of the data protection regulation. It is

however, it is not possible to provide deviating regulation regarding it

responsibility of the data controller to take appropriate technical and

organizational measures to ensure a level of security that is appropriate i

relation to the risk. This means that the National Board of Health and Welfare's regulations that 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 Swedish Data Protection Authority

can state that Karolinska University Hospital, in the capacity of

personal data controller, is responsible for these measures being taken.

As previously described, it is stated in article 24.1 of the data protection regulation one

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement partly aims to ensure that

the processing of the personal data is carried out in accordance with

the data protection regulation, partly that the person in charge of personal data must be able to

show that the processing of the personal data is carried out in accordance with

data protection regulation.

Security in connection with the processing 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 must be both technical and

organizational and they must ensure a level of security that is appropriate 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 for the rights and freedoms of the data subjects and assesses

the likelihood 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 meaning what kind of personal data is processed, how many

data, the question is, how many people process the data, etc.

Health care has a great need for information in its operations. The

it is therefore natural that the possibilities of digitization are utilized as much as possible

possible in healthcare. Since the Patient Data Act was introduced, one has a lot

extensive digitization has taken place in healthcare. As well as the data collections

size as how many people share information with each other has increased

substantially. This increase means at the same time that the demands on it increase

personal data controller, because the assessment what is an appropriate

safety is affected by the extent of processing.

It is also a matter of sensitive personal data. The data also concerns

people who are in a dependent situation when they are in need of care.

It is also often a question of a lot of personal data 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 that is processed must be protected against external actors as well

the business as against unauthorized access from within the business. It appears

of article 32.2 that the personal data controller, when assessing the appropriate

security level, in particular must take into account the risks of accidental or illegal

destruction, loss or for unauthorized disclosure or access. In order to

able to know what is an unauthorized access it must

personal data controller is clear about what constitutes an authorized access.

Needs and risk analysis

In ch. 4 § 2 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 assessment

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

national law prescribes requirements for an appropriate organizational measure that shall

is taken before assigning authorizations to the record system takes place.

A needs and risk analysis must partly contain an analysis of the needs, partly a

analysis of the risks based on an integrity perspective that may be associated

with an excessively wide allocation of authorization to access patient data.

Both the needs and the risks must be assessed based on the information that

need to be dealt with in the business, which processes are in question and

what risks exist for the individual's integrity.

The assessments of the risks need to take place based on organizational level, there

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

more sensitive to privacy than another, but also based on the individual level, if that is the case

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

that it is a matter of protected personal data, generally known persons or

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

the risk assessment. It appears from the preparatory work for the Patient Data Act that the more

comprehensive an information system is, the greater the variety

authorization levels there must be. (prop. 2007/08:126 p. 149). It is thus

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

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

updated.

In summary, the regulation requires that the risk analysis identifies

-

different categories of data (for example, data about health),

-

categories of data subjects (for example, vulnerable natural persons and

children), or

-

the extent (for example, the number of personal data and registered)

-

negative consequences for data subjects (e.g. 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 at

Processing of personal data. This also applies to internal confidentiality

as with coherent record keeping.

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

based on whether there are protected personal data that are

classified as confidential, information about publicly known people, information from

certain receptions or medical specialties (prop. 2007/08:126 p. 148149).

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

the risk to the rights and freedoms of the data subjects is and in any case determine

whether it is a question of a risk or a high risk (reason 76).

It is thus through the needs and risk analysis that it

data controller finds out who needs access, which

data the access possibility must include, at which times and in which

context the access is needed, and at the same time analyzes the risks to it

individual freedoms and rights that the processing may lead to. The result shall

then lead to the technical and organizational measures needed to

ensure that no other access than that which is necessary and

the risk analysis shows is justified should be able to take place.

When a needs and risk analysis is missing prior to granting authorization i

system, there is no basis for the personal data controller on a legal basis

way must be able to assign their users a correct authorization. The

personal data controller is responsible for, and must have control over, it

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

assign users a case of access to the record system, without this being established

on a performed needs and risk analysis, means that the personal data controller

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

the record system and also cannot show that he has the control that

is required.

When the Swedish Data Protection Authority has requested a needs and risk analysis has

Karolinska University Hospital referred to the steering document "Decision on

authorization assignment, guideline”4 (guidelines on authorization assignment) and

stated that it is the respective patient area and functional area manager
which must carry out and document needs and risk analyzes before
assignment of permissions. According to Karolinska University Hospital, it is done
when assigning authorizations, for example in case of new hires, on a regular basis
an investigation of the need for authorization that the employee also has
the template for needs and risk analyzes found in the guideline is not filled out
regularly. Karolinska University Hospital could at the time of
the inspection does not show any need and risk analysis carried out, but has
afterwards stated that they had started work to ensure that needs and
risk analyzes are carried out in the business. They have also submitted a documented
"needs and risk analysis" for the functional area Perioperative Medicine.
As indicated above, in a needs and risk analysis both the needs and
the risks are assessed based on the information that needs to be processed in
the business, which processes it is a question of and which risks to it
individual integrity that exists both organizationally and individually

4

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

level. It is thus a question of a strategic analysis at a strategic level, which
must provide an authorization structure that is adapted to the operations. It should
preferably result in instructions on authorization assignment but it is
not the instructions to the assigner of permissions which is the analysis.
At the time of the inspection, Karolinska University Hospital was unable to

demonstrate any needs and risk analysis. The later submitted needs and
the risk analysis regarding the Perioperative Medicine function does not meet
the data protection regulations' requirements for such an analysis according to ch. 4 § 2 HSLFFS 2016:40, as it constitutes a
general description of duties in
TakeCare for some specific occupational categories. The document contains none
analysis of which tasks the employees need to be able to perform their tasks
duties. The document does not contain an analysis of the risks that can
be associated with an excessively wide availability regarding different types of
personal data.
The Swedish Data Protection Authority further notes that the approach described in
permission assignment guidelines to analyze which permission which
to be assigned to an individual user is based on the existing ones
the authorization profiles. These are created based on what users need
be able to do with the tasks, for example read or write, and not from outside
which information about the patient that the individual user needs to have
access to in order to perform their work.
The needs and risk analyzes described in Karolinska University Hospital
guidelines on authorization assignment are not any analysis according to the requirements of a
needs and risk analysis according to 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 order.
The Swedish Data Protection Authority can thus state that Karolinska
The University Hospital's allocation of authorizations has not been preceded by one
necessary needs and risk analysis.
Authorization assignment regarding access to personal data about

patients

As has been reported above, a care provider may have a legitimate interest in having

a comprehensive processing of information about the health of individuals. Regardless of this shall

access possibilities to personal data about patients be limited to

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

Regarding the assignment of authorization for electronic access according to ch. 4.

§ 2 and ch. 6 Section 7 of the Patient Data Act, it appears from the preliminary works, prop.

2007/08:126 pp. 148-149, among other things that there must be different

authorization categories in the records system and that the authorizations should

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

authorization assignment should be considered an unwarranted spread of

journal data within a business and should not be accepted as such."

In healthcare, it is the person who needs the data 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 personal data controller finds out about whom

who needs access, which data the access should cover, at which

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

analyzes which risks to the individual's freedoms and rights are

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

organizational measures needed to ensure that no allocation

of authorization provides further access possibilities than the one that needs and
the risk analysis shows is justified. An important organizational action is to give
instructions to those who have the authority to assign permissions on how to do this
should go to and what should be taken into account so that, with the needs and risk analysis
as a basis, will be a correct authorization assignment in each individual case.
In addition to Karolinska University Hospital's guideline for the allocation of
authorizations, there is also a guidance document "Access to patient records,
guideline" (Access Guidelines), effective from 17 August 2018.5
However, the guidelines only provide a general description of the regulatory framework and
describes the prerequisites for the assignment of authorizations respectively for
to take part in the care documentation in TakeCare in different situations.
The Swedish Data Protection Authority states that even if each user de facto has
assigned an individual permission, the assigned permissions do 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
possibility of access to more personal data about patients or personal data
if more patients than he needs to carry out his work. They assigned
the permissions mean instead that the user has access to basically everything
personal data about patients in TakeCare. This is because there are only two
authorization profiles for nurses and doctors respectively, and there the only one

that differentiates the authorization profiles is that one
the nursing qualification has automated login to that care unit
the staff belongs and the one medical authorization has access to a so-called
emergency room. The limitation that otherwise appeared regarding
access possibilities to personal data in the records system refer to so-called
protected devices.
Datainspektionen considers against this background that, because the allocation
of authorizations not preceded by a necessary needs and risk analysis, not
there were conditions to limit assigned authorizations or there was support
to determine what are authorized access opportunities for executives
at Karolinska University Hospital.
That the assignment of authorizations has not been preceded by a need-and
risk analysis means that Karolinska University Hospital has not analysed
the users' need for access to the data, the risks that this access poses
can entail and therefore also not identified which access possibilities
which are justified for the users based on such an analysis. Karolinska
The University Hospital has therefore 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 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
confidentiality, partly within the framework of 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
approx. 2 million have been patients at Karolinska University Hospital.
Against the background of the above, the Swedish Data Protection Authority can state that

Karolinska University Hospital has processed personal data in violation of

article 5.1 f and article 32.1 0ch 32.2 of the data protection regulation by

Karolinska University Hospital has not limited the users

authorizations for access to the TakeCare records system to what only

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

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

Cape. Section 2 HSLF-FS 2016:40. This means that Karolinska University Hospital

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

5.2 of the data protection regulation, be able to demonstrate a suitable security for

the personal data.

Documentation of access in logs

The Swedish Data Protection Authority states that it is clear from the logs in TakeCare

information about the specific patient, which user has opened

the journal, actions 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 Swedish Data Protection Authority

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

accesses in the logs set up in the regulations of the National Board of Health and Welfare.

Choice of intervention

Legal regulation

If there has been a breach of the data protection regulation has

Datainspektionen a number of corrective powers to be available according to article
58.2 a - j of the data protection regulation. The supervisory authority can, among other things
order the personal data controller to ensure that the processing takes place in
in accordance with the regulation and if required in a specific manner and within a
specific period.
It follows from Article 58.2 of the data protection regulation that the Data Inspectorate i
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), depending
the circumstances of each individual case.
For authorities, according to Article 83.7 of the Data Protection Regulation, national
rules state that authorities can impose administrative penalty fees.
According to ch. 6 § 2 of the Data Protection Act, penalty fees can be decided for
authorities, but to a maximum of SEK 5,000,000 alternatively SEK 10,000,000

depending on whether the violation relates to 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 deciding whether a
administrative penalty fee shall be imposed, but also what shall affect
the amount of the penalty fee. Of central importance for the assessment of
the seriousness of the breach is its nature, severity and duration. If
it is a question of whether a minor violation gets the supervisory authority, according to reason
148 of the Data Protection Regulation, issue a reprimand instead of imposing one
penalty fee.

Health care has, as mentioned, a great need for information in its
business and in recent years has had a very extensive digitization
occurred in healthcare. Both the size of the data collections and how many there are
share information with each other has increased significantly. This increases the demands on
the personal data controller, because the assessment what is an appropriate
safety is affected by the extent of processing.

In healthcare, this means an 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 finely divided. The
is therefore essential that there is a real analysis of the needs based on different
operations and various executives. Equally important is that it happens
actual analysis of the risks that may arise from an integrity perspective
in case of an excessive when assigning authorization to access. Based on this analysis
the individual executive's access must then be restricted. This one
authorization must then be followed up and changed or restricted accordingly
which changes in the duties of the individual executive provide
reason for it.

The Data Inspectorate's supervision has shown that Karolinska University Hospital does not
have taken appropriate security measures to provide protection to
the personal data in the records system by Karolinska
The University Hospital, in its capacity as a personal data controller, has not followed the requirements
as stated in the Patient Data Act and the regulations of the National Board of Health and Welfare. Karolinska
The University Hospital has thereby failed to comply with the requirements in Article 5.1 f
and article 32.1 and 32.2 of the data protection regulation. The omission includes

as well as the internal secrecy according to ch. 4. the patient data act as it

coherent record keeping according to ch. 6 the patient data act.

The Swedish Data Protection Authority therefore orders, with the support of 58.2 d i

data protection regulation, Karolinska University Hospital to ensure that

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

within the framework of the internal secrecy as well as within the framework of it

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

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

the risk analysis, assign each user individual authorization for access to

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

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

Penalty fee

The Data Inspectorate can state that the violations basically refer to

Karolinska University Hospital's obligation to take appropriate measures

security measures to provide protection for personal data according to

data protection regulation.

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

personal data and extensive permissions. The caregiver needs to

necessity to have extensive processing of information about individuals' health.

However, it must not be unrestricted, but must be based on what individuals do

employees need to be able to perform their tasks. The Swedish Data Protection Authority

states that it is a matter of data that includes direct identification

of the individual through both name, contact details and social security number,

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

information about, for example, family relationships, sex life and lifestyle. The patient

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

nature, extent and the patients' dependency status give caregivers a

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

personal data.

Further aggravating circumstances are that the treatment of

patient data in the master record system is at the core of a healthcare provider's

business, that the treatment covers many patients and the possibility of

access refers to a large percentage of employees. In this case it is about

about 2,000,000 patients within the framework of the internal secrecy and

around another 1,000,000 patients within the scope of the combined

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

the data is not accessible to the users outside these devices.

The Swedish Data Protection Authority can also state that Karolinska

The University Hospital has not followed the Data Inspectorate's previous order from

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

basis for the allocation of authorizations according to the then requirement in ch. 2. 6

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

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

circumstance, according to article 83.2 e of the data protection regulation.

The deficiencies that have now been identified have thus been known to Karolinska

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

intentional and thus considered more serious.

When determining the seriousness of the violations, it can also be established that

the violations also include the fundamental principles of Article 5 i

the data protection regulation, which belongs to the categories of more serious

Violations that may result in a higher penalty fee according to Article 83.5 i

data protection regulation.

Taken together, these factors mean that the violations cannot be assessed

as minor infractions without infractions that should lead to one

administrative penalty fee.

The Swedish Data Protection Authority believes that these violations are closely related to

each other. That assessment is based on the fact that the needs and risk analysis must

form the basis for the assignment of the authorizations. The Swedish Data Protection Authority

therefore considers that these violations are so closely related to each other

that they constitute connected data processing according to Article 83.3 i

data protection regulation. The Swedish Data Protection Authority therefore determines a joint

penalty fee for these violations.

The administrative penalty fee must be effective, proportionate and

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

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

effect and that it is also proportionate in relation to current as well

violations as to the solvency of the subject of supervision.

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

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

data protection regulation.

In light of the seriousness of the violations and that the administrative

the penalty fee must be effective, proportionate and dissuasive

the Data Inspectorate determines the administrative penalty fee for

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

This decision has been made by the director general Lena Lindgren Schelin after

presentation by IT security specialist Magnus Bergström. At the final

Chief legal officer Hans-Olof Lindblom, the unit managers are also involved in the handling

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 the attention of:

Data Protection Officer

How to appeal

If you want to appeal the decision, you must write to the Swedish Data Protection Authority. Enter in

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

The appeal must have been received by the Swedish Data Protection Authority no later than three weeks from

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

the Swedish Data Protection Authority forwards it to the Administrative Court in Stockholm for

examination.

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain

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

secrecy. The authority's contact details appear on the first page of the decision.

2 8 (28)