Decision

Diarienr

2020-12-02

DI-2019-3845

Digital Medical Supply Sweden AB (KRY)

Torsgatan 21

113 21 Stockholm

Supervision under the Data Protection Regulation and

Patient Data Act - needs and risk analysis and

questions about access in journal systems To Digital

Medical Supply Sweden AB (KRY)

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

Content

The Data Inspectorate's decision 3

Report on the supervisory matter 4

What has emerged in the case 5

Personal data controller 5

Operation..... 5

Journal system 5

Users and patients 5

Internal privacy 6

Needs and risk analysis 6

Authorization of access to personal data 9

Consolidated record keeping 10

Needs and risk analysis 10

Authorization of access to personal data about

patients 10

Documentation of access (logs) 11

Grounds for the decision 12

Applicable rules..... 12

The Data Protection Regulation the primary source of law 12

The Data Protection Regulation and the relationship with complementary national

regulations 13

Supplementary national provisions 14

Requirement to do needs and risk analysis 15

Internal privacy 16

Consolidated record keeping 16

Documentation of access (logs) 17

The Data Inspectorate's assessment 17

Responsibility of the data controller for security 17

Needs and risk analysis 18

Authorization of access to personal data about patients 23

Documentation of access (logs) 25

Choice of intervention 25

Legal regulation 25

Assessment of whether a penalty fee should be imposed 26

Order..... 28

How to appeal..... 30

The Data Inspectorate's decision

During an on-site inspection on April 4, 2019, the Data Inspectorate has established that

Digital Medical Supply Sweden AB (KRY) processes personal data in violation

with Article 5 (1) (f) and (2) and Article 32 (1) and (2) of the Data Protection Regulation1

by

1.

KRY has not carried out needs and risk analyzes that meet

the requirements according to the provisions in ch. 4 § 2 and ch. 6 § 7

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

regulations and general advice on record keeping and processing of

personal data in health care (HSLF-FS 2016: 40) before

allocation of permissions takes place in the journal system ProReNata and

National patient overview. This means that KRY is not in sufficient

to the extent that it has taken appropriate organizational measures to:

be able to ensure and be able to show that the treatment of

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

the risks.

2. KRY has not shown that KRY has restricted users' permissions for

access to the ProReNata medical record system and the National Patient Overview

limited to what is only needed for the user to be able to

perform their duties in health care accordingly

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

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

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

Data Protection Regulation).

1

with ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and Chapter 4 2 § HSLFFS 2016: 40. This means that KRY has not

taken sufficient

measures to ensure and demonstrate appropriate security

for personal data.

The Data Inspectorate states that KRY since the inspection on April 4, 2019

has improved its needs and risk analyzes but that the analyzes are not in all

parts meet the requirements that apply according to ch. 4 § 2 and ch. 6 § 7

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

general advice on record keeping and processing of personal data in health and medical care (HSLF-FS 2016: 40).

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

the data protection ordinance KRY to supplement by the last February 2021

the needs and risk analyzes for the journal systems ProReNata and Nationell

patient overview by developing the analysis of the risks for those registered

rights and freedoms and that thereafter, with the support of needs and

the risk analyzes, make a reassessment regarding the allocation of

permissions so that each user has access to only those

personal data needed for the user to be able to fulfill his

duties in health care, in accordance with Article 32 (1) and

32.2 of the Data Protection Ordinance, Chapter 4 § 2 and ch. 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 the inspection by letter dated 22 March 2019 and

has on site on April 4, 2019 reviewed KRY's decision on the allocation of

authorizations have been preceded by a needs and risk analysis. Supervision has also

included how KRY assigned permissions for access to

the main medical record system ProReNata and the National Patient Overview and which

access opportunities the granted privileges provide within both the framework of

the internal secrecy according to ch. the Patient Data Act, as the cohesive one

record keeping according to ch. 6 the Patient Data Act. In addition to this has

The Data Inspectorate also examined the documentation of access (logs)

contained in the journal system.

The Data Inspectorate has only examined users' access to

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

part of and read. Supervision does not include the functions included in

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

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

What has emerged in the case

KRY has mainly stated the following.

Personal data manager

KRY is the care provider and personal data manager.

Operation

KRY conducts care via video meetings, so-called video care, which is done by the patient downloads the app KRY. KRY is the technical platform and also the brand that KRY uses externally towards patients. The app is available for mobile devices with the operating systems iOS or Android.

It is KRY's parent company Webbhälsa AB (hereinafter Webbhälsa) that has developed the app and which handles the operation of the technical platform. Web Health owns the KRY brand, develops the technology and services the care provider KRY with licenses. There are two separate legal units but the staff is sitting together in the same office.

There are historical reasons behind the fact that there are two companies but one Operation. When KRY was created, Web Health turned to regions and county council to offer the service, but it took a long time to get caregivers to start using the service. That is why Webbhälsa started the company KRY as one own care provider that conducts care via the app KRY.

Journal system

KRY has stated that the record system used by KRY is called ProReNata and has been used since the business started in March 2016. For cohesive record keeping, the National Patient Overview (NPÖ) system is used.

Users and patients

At the time of the inspection, there were 490 people with access to ProReNata. On April 8, 2019, the total number of patients was registered in ProReNata 450 331.

Internal secrecy

Needs and risk analysis

During the inspection and subsequent review have essentially the following

arrived.

During the inspection on April 4, 2019, the Data Inspectorate took in a needs and

risk analysis dated 11 March 2019. On 10 May 2019, KRY submitted a

revised needs and risk analysis dated 2 May 2019 where also cohesive

record keeping is included but which otherwise mainly contains the same needs and risk analysis as the document dated 11

March 2019. 20 March 2020

KRY came in with a new revised version dated March 1, 2020 that contains

a largely revised analysis.

The needs and risk analysis dated 11 March 2019 includes one

description of needs in the business, risks and risk management.

The document states, among other things, the following regarding needs in the business for

health care professionals:

Due to the business' medical focus, digital nature and absence of physical

presence in different geographical areas, health and medical staff at KRY are organized in

a single staff pool scheduled by administrative staff for meetings with all types of

patients. Healthcare professionals are thus not organized solely based on

necessary competence in the individual case (eg general practitioner, nurse or psychologist),

scheduling and availability. Although some type of treatment, e.g. treatment of children

under 6 months of age or treatment of certain symptoms typical of e.g. women, should be cared for

by certain specialized staff, the work of this staff is not limited to these symptoms then

they also meet other types of patients. In the event that KRY care operations change over time,

by e.g. a larger number of available staff, several different categories of healthcare staff or

care processes (such as specialist care), an updated needs and risk analysis will

carried out to ensure patient safety but also to ensure respect for the patient

integrity is constantly observed.

To ensure good quality, availability and cost efficiency, it is of utmost importance that staff who participate in the actual care within the framework of KRY outpatient care and in a patient relationship, has a good and sufficient knowledge of the patient's medical history. All clinics and relevant administrative staff (such as medical secretaries who have relevant training for his assignment) hired by KRY may meet all patients who apply care via KRY and may then participate in the care of these and thus need access to the patient's medical record in order to be able to perform their duties.

In summary, it is KRY's assessment that it is both the nature of the business and unique distinctiveness there is a great need not to limit eligibility for medical and relevant administrative staff to certain geographically or demographically delimited patient groups in the current situation. For other types of authorizations, there is a more limited need in accordance with what as stated above.

Under the heading "risks" it is stated that KRY sees a number of risks with a broad authorization and states that the risks in KRY's view are primarily:

- Unauthorized access for healthcare professionals or relevant administrative staff due to ignorance of rules and procedures on confidentiality and patient safety;
- Unauthorized access for healthcare professionals or relevant administrative staff as a result of mistakes or otherwise due to human factor;

- Unauthorized access for healthcare professionals or relevant administrative staff as a result of deliberate abuse;
- Unauthorized access for third parties due to health and healthcare professionals or relevant administrative staff lose equipment or, knowingly or unknowingly, sharing login information to systems; and
- Unauthorized access by third parties due to data breaches.

Under the heading "risk management" it is stated that KRY's assessment is that they risks arising from a broad authorization allocation can be significantly limited and to an acceptable level through the organizational and technical safety measures taken by KRY, which mainly include:

- Recruitment routines, including background checks, to minimize the risk of inappropriate individuals being given access to personal data about patients;
- Routines for onboarding, which i.a. includes guidance and training on the use of systems, equipment, relevant statutes and routines regarding confidentiality and patient safety to raise awareness of obligations, rights and responsibilities;
- Signing of a reminder of confidentiality and / or confidentiality commitments for to preventively reduce the risk of unauthorized access and to increase

knowledge of confidentiality and patient safety;

Use of equipment provided and controlled by

KRY;

Procedures for assigning, modifying and removing permissions for

to preventively minimize the risk that authorizations are not adequate

over time;

Technical tools to preventively minimize the need for beatings in

the record system and thus the risk of illegal access, e.g. like one

results of mistakes or insufficient knowledge. In health and

healthcare professionals' work for digital care, will only be relevant

patient be available. In this system, no other patient than it can

which the meeting concerns to be opened. To be able to search for other patients

current personnel must actively make an unauthorized strike;

Obtaining patient approval before medical

secretaries make beatings in patient records; and

Clear information to relevant staff and routine for logging and

control in order to prevent employees from refraining from unauthorized use

access and to reactively detect and follow up on such

access. All journal openings that are not connected to one

active care relationship / performed patient meeting is logged and reviewed

manually.

Under the heading "conclusions" it is stated, among other things:

A broad competence for medical and administrative staff for patients

journals are therefore justified under current conditions in KRY to

be able to provide patient-safe care, provided that KRY operates one

continued effective security work to identify, evaluate and manage

risks in their business.

However, this conclusion needs to be reconsidered regularly and may come to

changes as KRY grows, changes medical orientation, develops

their business concept and in other similar circumstances. One

condition for being able to limit eligibility for different clinics, is that we

despite this can ensure accessibility for patients. A division between

clinics for which group of patients one has, presupposes a significant

greater staff than the one currently available for KRY, but is one

desirable goal to aim for in the long run.

In the second revision dated March 1, 2020, KRY has largely reworked

analysis and identified risks based on certain types of data and

patient groups in the form of information on persons with a protected identity,

public figures, employees and staff's own tasks. Further has

KRY in the revised analysis also assessed probability and consequence for

the identified risks. The analysis also contains more detailed information

review of the need for access for the various categories of staff. To

Unlike the previous versions of the analysis, KRY has come to the conclusion

that a narrow qualification is sufficient for doctors, nurses and psychologists,

except so-called plus doctors, plus psychologists and doctors on call. The tight

the authorization is stated to mean that users can only access information

about patients (both internal medical records and NPÖ) at patient meetings. Further

stated that access is granted in connection with the staff is scheduled with

patient and is automatically withdrawn 4 months after access has been granted

and that before meeting with patient has taken place can not beat on such patient

happen.

Authorization assignment for access to personal data

During the inspection, the following mainly emerged.

Clinical staff, at the time of inspection, doctors, nurses and

psychologists and administrative staff in the form of medical secretaries, have

actual access to all data in all patient records in ProReNata. The

there are limitations in the form of organizational and technical controls, which

according to KRY has been an important part of the assessment of authorization management there

KRY thought about what other security can be offered.

KRY systematically reviews all journal accesses. All access is reviewed and

matched against whether clinics had a meeting with the patient that day. In another

In this case, access is flagged and reviewed to see if there is another reasonable one

explanation of access. There is a check every four weeks for

active accounts (by reviewing the personnel schedule). If, for example, one

doctor does not have a passport booked for the next four weeks so is disabled

doctor's account. If a doctor with an inactive account has a passport they have entered

over the next four weeks, the account is activated.

The design of the permissions is based on the digital character of
the service that KRY offers, that care has a general focus and is not
specialized, that patients are spread across the country, that the queue time for
the patient should be as short as possible and that the staff is organized in one
only staff pool. A patient who calls in gets help from a doctor one day and
a completely different doctor the next day, and the doctors can sit in completely different places in

Sweden. According to KRY, this requires that doctors must be able to see each other
journal information to be able to provide good care.
KRY has made the assessment that all information available about the patients is
relevant to the healthcare staff, but KRY is aware that this may happen
to change as the organization grows.
In the needs and risk analysis dated 1 March 2020, KRY has done one more
detailed analysis of the need for access to data in ProReNata based on those
tasks of different categories of staff and concluded that a narrow
eligibility is sufficient for doctors, nurses and psychologists in that way
as described in the section above in the account of the revised needs and
risk analysis.
Coherent record keeping
During the inspection and subsequent review have essentially the following
arrived.
Needs and risk analysis
During the inspection, there was no special needs and risk analysis for access to
NPÖ. KRY has submitted two revised needs and risk analyzes

dated 2 May 2019 and 1 March 2020 which includes the use of national

patient overview (NPÖ) in the operation. The needs and risk analysis dated 2

May 2019 otherwise contains essentially the same needs and risk analysis as

the document dated March 11, 2019.

In the needs and risk analysis dated 1 March 2020, KRY has done one more

detailed analysis of the need for access to data in NPÖ based on the various

the tasks of the staff categories.

Authorization of access to personal data about patients

KRY has stated that the care provider is part of a system for cohesion

record keeping through NPÖ as a "consumer". This means that the staff at

KRY can take part in the information in NPÖ, but KRY "produces" (makes available)

no own information in NPÖ.

At the time of the inspection, it emerged that all staff had access

to ProReNata also had access to NPÖ.

The revised needs and risk analysis dated 1 March 2020 shows that

all personnel who have access to ProReNata as a starting point do not have one

need for access to data in NPÖ. Nurses and

care administrators are stated as a starting point to have a need for access to

ProReNata but not to NPÖ.

Documentation of access (logs)

KRY has stated the following.

For each strike in ProReNata, a log message is created with information

about which staff at a given time made a strike. Time

refers to both date and time. It is clear which patient it is,

the identity of the user, what action the user has taken, for example

signing, taking notes and reading. Because KRY is not organized in several

different care units, only one unit appears that is the same for all

staff.

There are three different types of logs in ProReNata; visitor logs, server logs

and event logs. Visitor log shows when a user visited a journal and

when it left the journal. Server log shows when the system has registered one

server calls to a journal and can mean that users have read but also

other reasons. Event log shows logged system events that affect one

user or patient, for example read, written or signed.

Access to NPÖ is logged by Inera and is available to administrators at

KRY.

After the inspection, KRY has noted that the specific measure

note cancellation (not signed) is not logged separately in ProReNata.

KRY has raised this with ProReNata AB, which at KRY's request has

developed such logging. Shreds of notes will also come

because to be logged from 16 May 2019 in order to give KRY even better

opportunities to follow up and ensure good and safe care.

Justification of the decision

Applicable rules

The Data Protection Regulation is the primary source of law

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

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

also applies to health care.

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

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

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

in a way that ensures appropriate security for personal data,

including protection against unauthorized or unauthorized treatment and against loss;

destruction or damage by accident, using appropriate

technical or organizational measures.

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

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

the principles set out in paragraph 1 are complied with.

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

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

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

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

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

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

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

if necessary.

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

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

of the latest developments, implementation costs and treatment

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

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

take appropriate technical and organizational measures to ensure a

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

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

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

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

the personal data transferred, stored or otherwise processed.

Recital 75 states that in assessing the risk to natural persons

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

personal data covered by professional secrecy, health data or

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

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

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

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

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

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

on the basis of an objective assessment, which determines whether

the data processing involves a risk or a high risk.

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

the meaning of the Data Protection Regulation's requirements for security in

Processing of personal data.

The Data Protection Regulation and the relationship with complementary national

provisions

According to Article 5 (1) (a) of the Data Protection Regulation, personal data must:

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

legal basis by at least one of the conditions of Article 6 (1) being met.

The provision of health care is one such task of general

interest referred to in Article 6 (1) (e).

In health care, the legal bases can also be legal

obligation in Article 6 (1) (c) and the exercise of authority under Article 6 (1) (e)

updated.

When it comes to the legal bases legal obligation, in general

interest or exercise of authority by the Member States, in accordance with Article

6.2, maintain or introduce more specific provisions for adaptation

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

National law may lay down specific requirements for the processing of data

and other measures to ensure legal and fair treatment. But

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

duty; Article 6 (3) states that the basis for the treatment referred to in

paragraph 1 (c) and (e) shall be determined in accordance with Union law or

national law of the Member States. The legal basis may also include

specific 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).

The supplementary provisions in the Patient Data Act aim to:

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

thus through the regulation made a balance in terms of how

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

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

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

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

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

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

personal data in health care.

National provisions that supplement the requirements of the Data Protection Regulation

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

2016: 40.

Requirement to do needs and risk analysis

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

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

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

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

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

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

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

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

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

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

eligibility assignments based on analyzes of which details are different

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

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

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

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

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

may require special risk assessments.

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

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

categories of healthcare professionals for electronic access to data in

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

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

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

dissemination of medical records within an

not accepted.

Furthermore, data should be stored in different layers so that more sensitive data require active choices or

otherwise not as easily accessible to staff as less sensitive tasks. When it

applies to staff who work with business follow-up, statistics production, central

financial administration and similar activities that are not individual-oriented, it should be

most executives have enough access to information that can only be indirectly derived

to individual patients. Electronic access to code keys, social security numbers and others

data that directly point out individual patients should be strong in this area

limited to individuals.

Internal secrecy

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

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

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

Coherent record keeping

The provisions in ch. 6 the Patient Data Act concerns cohesive record keeping,
which means that a care provider - under the conditions specified in § 2 of the same
chapter - may have direct access to personal data processed by others
caregivers for purposes related to care documentation. The access to
information is provided by a healthcare provider making the information about a patient
which the care provider registers if the patient is available to other care providers
who participate in the coherent record keeping (see Bill 2007/08: 126 p. 247).

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

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

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

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

record keeping.

Documentation of access (logs)

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

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

automatically documented and systematically checked.

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

1. 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 previously described, Article 24 (1) of the Data Protection Regulation provides a

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement is partly to ensure that

the processing of personal data is carried out in accordance with

the Data Protection Ordinance, and that the data controller must be able to

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

the Data Protection Regulation.

The safety associated with the treatment is regulated more specifically in the articles

5.1 f and 32 of the Data Protection Regulation.

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

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

The health service has a great need for information in its operations. The
It is therefore natural that the possibilities of digitalisation are utilized as much as
possible in healthcare. Since the Patient Data Act was written, one has 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 and the data 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 and every one
the data may over time be processed by very many people.

All in all, this places great demands on the person responsible for personal data.

The data processed must be protected from outside actors as well

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

It should be noted that Article 32 (2) states that the controller, at

assessment of the appropriate level of safety, in particular taking into account the risks of

unintentional or unlawful destruction, loss or unauthorized disclosure or

unauthorized access. To be able to know what is an unauthorized access must

the data controller must be clear about what is an authorized access.

Needs and risk analysis

The National Board of Health and Welfare's regulations that supplement the Patient Data Act contain it

stated in ch. 4 § 2 HSLF-FS 2016: 40, that the care provider shall make a needs and

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

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

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

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

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

with an overly allotment of access to personal data

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

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

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

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

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

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

the issue of, for example, protected personal data, generally known persons

or otherwise particularly vulnerable persons. Also the size of the system

affects the risk assessment. The preparatory work for the Patient Data Act states that

the more comprehensive an information system is, the greater the variety

eligibility levels must exist (Bill 2007/08: 126 p. 149).

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

an authorization structure that is adapted to the business and this should

kept up to date.

In summary, the regulation requires that the risk analysis identify

- different categories of 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 based on

the nature, scope, context and purpose of the treatment (recital 76).

It is thus through the needs and risk analysis that it

personal data controller finds out who needs access, which

data access 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 there is no access other than that which is needed 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 during the inspection requested a documented

needs and risk analysis, KRY submitted a document dated 11 March 2019

with the heading "Authorization allocation Needs and risk analysis". KRY has thereafter, on 10 May 2019, KRY submitted a revised needs and risk analysis dated 2 May 2019, which also includes coherent record keeping but which otherwise essentially contain the same needs and risk analysis as the document dated 11 March 2019. On 20 March 2020, KRY submitted a new one revised version dated March 1, 2020 which contains a largely revised analysis.

In the needs and risk analysis from 11 March 2019, KRY has carried out an analysis regarding internal confidentiality where the need for access to personal data in the journal system has been weighed against risks that KRY considers to follow access rights. It appears that the purpose is to land based on the analysis in a model for authorization allocation in the business. In the analysis, KRY identified and described the need for access based on how KRY conducts its Operation. Furthermore, KRY has identified and described needs based on different duties of staff categories. KRY has come to a conclusion after that

have weighed the need against the risks identified by KRY and the measures taken to reduce the risks.

The Data Inspectorate can state that KRY has carried out a needs and risk analysis that identifies and analyzes needs and risks. The analysis is implemented at strategic level and shall form a basis for the business authorization. The needs and partly also the risks are analyzed based on the actual conditions in the business. KRY has based on it analysis that has been carried out identified technical and organizational measures

to reduce the risk of unauthorized access.

In its initial analysis, however, KRY has not taken into account how negative consequences for data subjects, different categories of data, categories of registered, or the extent of the number of personal data and registered, affects the risk to the rights and freedoms of natural persons at KRY's processing of personal data in ProReNata and National Patient Overview. There are also no special risk assessments based on whether there are e.g. protected personal data that is classified, confidential information celebrities, information from certain clinics or medical specialties or other factors that require special protective measures. The there is also no assessment of how likely and serious the risk is for them data subjects' rights and freedoms are judged to be.

KRY has thus taken measures that are likely to reduce the risk of physical rights and freedoms of persons. However, the needs are too general analyzed and the risks to the data subjects' rights and freedoms are not in adequately identified and assessed. Among other things, a deeper one is missing analysis of the risks to the individual's integrity based on different categories of data as different categories of data subjects.

In summary, the Data Inspectorate states that KRY at carried out a needs and risk analysis at strategic level, but that it does not meet the requirements of the data protection regulations such analysis because KRY has not considered the risks, of varying probability and seriousness, for the rights and freedoms of natural persons and not taken into account the different types of risks to the privacy of the individual that may be associated with an overly accessible on certain types of data.

The Data Inspectorate states that KRY thereby at the time of the inspection

has not carried out a needs and risk analysis that meets the requirements that

set in

Chapter 4 § 2 HSLF-FS 2016: 40, neither within the framework of internal secrecy

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

Chapter 6 the Patient Data Act. This means that KRY has not taken appropriate

organizational measures in accordance with Article 5 (1) (f) and Article 31 (1) and (2) for

be able to ensure and, in accordance with Article 5 (2), be able to demonstrate that

the processing of personal data has a security that is appropriate in

in relation to the risks.

KRY has supplemented with a needs and risk analysis dated 1 March

2020. In the new needs and risk analysis, KRY has largely reworked

analysis and identified risks based on certain types of data and

patient groups in the form of information on persons with a protected identity,

public figures, employees and staff's own tasks. Further has

KRY in the revised analysis also assessed probability and consequence for

the identified risks. The analysis also contains more detailed information

review of the need for access for the various categories of staff.

Unlike the previous versions of the analysis, KRY has emerged

that a narrow qualification is sufficient for doctors, nurses and psychologists,

except so-called plus doctors, plus psychologists and doctors on call. The tight

the authorization is stated to mean that users can only access information

about patients (both internal medical records and NPÖ) at patient meetings. Further

stated that access is granted in connection with the staff is scheduled with

patient and is automatically withdrawn 4 months after access has been granted

and that before meeting with patient has taken place can not beat on such patient

happen.

The Data Inspectorate can state that the new needs and risk analysis

contains an in-depth needs analysis where both organization, different

occupational categories and different tasks have been taken into account. Concerning

the risk assessment, it is also in-depth and at least takes into account different

categories of registered. It also includes an assessment of how likely

or the serious risk to the data subjects' rights and freedoms is. KRY has

based on the new roles created more limited access opportunities.

Based on its special activities, KRY does not have such a complex organization that

further needs assessments are required. As for the risks so

they are still not analyzed on the basis of categories of data. Tasks

which can be perceived as more privacy-sensitive are, for example, information such as

concerns sexual life, substance abuse, mental illness or threats or violence especially if it is in

close relations. Even the analysis based on categories of registered can

deepened by the categories that are actually dealt with in the business

undergone. The fact that the business has a homogeneous structure means that it will be

even more important to analyze these risks and assess if and how they can

be remedied because such a large proportion of staff need to be assigned the same type

of access.

Authorization allocation for access to personal data about patients

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

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

access to personal data about patients may be limited to

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

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

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

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

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

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

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

unauthorized dissemination of journal information within a business and should as

such is not accepted. "

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

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

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

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

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

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

analyzes the risks to the individual's freedoms and rights

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

organizational measures needed to ensure no allocation

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

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

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

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

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

It appears that KRY at the time of the inspection had not limited

health professionals and medical secretaries

access to patient data either within its framework

internal confidentiality of the ProReNata medical record system, or within the framework of

coherent record keeping in the journal system NPÖ. KRY, on the other hand, had

introduced measures to avoid unauthorized access, including in the form of

logging and manual review of all journal openings that were not

linked to an active care relationship or performed patient meeting and deactivation

of accounts every four weeks for doctors without passports booked the next four

the weeks.

Because the needs and risk analysis that KRY had carried out

the time of the inspection did not take sufficient account of

the risks to the rights and freedoms of natural persons or the different kinds

risks that may be associated with an overly availability regarding

certain types of information, KRY has not shown that the reading permissions have been restricted

in the manner required by the Data Protection Ordinance and the Patient Data Act.

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. KRY

has, through subsequent measures taken, reduced that risk by improving

analyzes and subsequent measures taken.

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

the time of the inspection has processed personal data in violation of Article 5 (1) (f)

and Article 32 (1) and (2) of the Data Protection Regulation by KRY, in accordance with

with Article 5 (2) and (1), have not been able to show that KRY has restricted users

permissions for access to the journal system ProReNata and National

patient overview to what is only needed for the user to be able to

fulfill their duties in health care according to ch. § 2 and

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

The needs and risk analysis dated 1 March 2020 shows that KRY has introduced

restrictions on access to personal data about patients. Unlike

the previous versions of the analysis, KRY has come to the conclusion that a narrow

eligibility is sufficient for doctors, nurses and psychologists, except so-called

plus doctors, plus psychologists and doctors on call. The narrow authority

is stated to mean that users can only access information about patients

(both internal medical records and NPÖ) at patient meetings. It is further stated that access

assigned in connection with the staff is scheduled with the patient and drawn

automatically returned 4 months after access was granted and that before

meeting with patient has taken place, beating on such patient can not take place.

KRY has thus improved the restriction of access since the inspection.

As stated in the section above regarding the new needs and

However, the risk analysis still requires some additions to the analysis

must be comprehensive and be able to show that access has been restricted accordingly

with the requirements of the Data Protection Ordinance and the Patient Data Act. From

the result of these additions must then KRY assess its model for

authorization.

Documentation of access (logs)

The Data Inspectorate can state that from the logs in ProReNata and NPÖ

information on which staff made one at a given time

beating. Time refers to both date and time. It is clear which

patient it concerns, the user's identity, what the user has taken for

action, such as signing, taking notes, and reading. Because KRY is not

organized in several different care units, only one unit appears

the same for all staff.

After the inspection, KRY has noted that the specific measure

note cancellation (not signed) is not logged separately in ProReNata

but that KRY has stated that such logging has been introduced as of the 16th

May 2019. The Data Inspectorate notes that the documentation of the access

(the logs) in ProReNata and NPÖ are now in accordance with the requirements

which appears from ch. 4 9 § HSLF-FS 2016: 40.

Choice of intervention

Legal regulation

If there has been a violation of the Data Protection Regulation

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

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

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

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

specific period.

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

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

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

the circumstances of each individual case. The overall starting point for

imposition of a penalty fee is that in the individual case it is judged to be

effective, proportionate and dissuasive (cf. Article 83 (1)).

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.

Assessment of whether a penalty fee should be imposed

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 written, one has 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.

In this context, it 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 even more

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

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

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

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

this analysis must then be restricted to the individual executive.

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

hand that changes in the individual executive's duties

reason for it.

The Data Inspectorate has found that KRY at the Data Inspectorate's inspection

carried out a needs and risk analysis at a strategic level, but that the analysis

not fully taken into account the risks, of varying degrees of probability and severity, for

the rights and freedoms of natural persons and that KRY has not taken different considerations into account

kind of risks to the privacy of the individual that may be associated with one

too in the availability of certain types of information. KRY then has in

March 2020 performed a new needs and risk analysis. The new needs and

the risk analysis goes deeper than the previous one and takes into account both organization and

different occupational categories and tasks. The risk assessment is also that

in-depth and now also includes an assessment of probability and

seriousness of risks to data subjects' fundamental freedoms and rights.

Although the needs analysis can now be considered acceptable, it is missing

still parts relating to the risk assessment. What needs closer

remedied, the Data Inspectorate describes below under the heading injunction.

The Data Inspectorate's inspection has thus shown that KRY has not met the requirement

to take appropriate security measures to protect the personal data in

the journal systems by not having fully complied with the requirements that follow

the Patient Data Act and the National Board of Health and Welfare's regulations on conducting needs and risk analysis, before

the allocation of authorizations in the system takes place. Thereby
KRY has also not been able to show that KRY has limited the authorization for
access to only what is needed for the individual to be able to fulfill
their duties in health care. This means that KRY does not
has also complied with the requirements of Article 5 (1) (f) and Article 32 (1) and (2) (i)
the Data Protection Regulation. The lack of compliance with the rules includes both
the internal secrecy according to ch. the Patient Data Act as the cohesive one
record keeping according to ch. 6 the Patient Data Act.
The Data Inspectorate can state that the violations are the starting point
serious in terms of provisions that are fundamental to ensuring that
the processing of personal data is subject to adequate security measures
to protect the data subjects' fundamental freedoms and rights. Also
the nature of the data, the number of data subjects concerned, which in this case amounts to
about
450,000 patients, as the number of employees and the availability of a large proportion of them
employees to these patients' tasks speak in aggravating direction.
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.
It is thus typically not a question of minor infringements but
infringements which should normally lead to an administrative penalty fee.

When assessing whether a penalty fee should be imposed, it must be considered at the same time
if it is required, taking into account that it is a question of a measure as in it
individual case is effective, proportionate and dissuasive.
As stated, at the time of the inspection, KRY had carried out a needs and risk analysis at a strategic level and taken measures
that were likely to
reduces the risk to the rights and freedoms of natural persons. KRY has thus
tried to comply with the requirements for the processing of personal data and has
to a not insignificant extent taken measures in order to comply with the requirements and
reduce the risks. The Data Inspectorate assesses that KRY's lack of compliance
has not meant that the data subjects have been deprived of protection of their rights
and freedoms to the same extent as if none or only deficient
measures had been taken.
KRY has also taken measures itself to try to come to terms with
shortcomings in the needs and risk analysis after the Data Inspectorate's inspection by
to establish and submit to the Data Inspectorate two revised needs and risk analyzes. It should also be taken into account that
KRY itself has drawn attention
lack of logging and taken steps to address that shortcoming.
In a weighted assessment, the Data Inspectorate finds that they are relevant
the infringements are admittedly typically of such a nature that a
administrative penalty fee should normally be imposed but that in the case
the case is not proportionate to such an intervention by
The Data Inspectorate. KRY should instead be ordered to take measures to ensure
that the processing takes place in accordance with the Data Protection Regulation.
Order
When deciding on an injunction, the Data Inspectorate considers the revisions of
the needs and risk analysis that KRY has done after the inspection.

During the supervision case, KRY has revised its needs and

risk analysis on two occasions. The first revision was made on 2 May 2019 and

the second revision was made on March 1, 2020. Through the first revision

adjusted the KRY analysis to also include coherent record keeping in

NPÖ. In the second revision, KRY has largely reworked the analysis and

identified risks based on certain types of data and patient groups in form

of data on persons with a protected identity, public figures,

employees and the staff's own tasks.

Furthermore, in the revised analysis, KRY has also assessed probability and

consequence of the identified risks. The analysis also contains more

detailed review of access needs for the various

staff categories. Unlike the previous versions of the analysis

KRY has come to the conclusion that a narrow qualification is enough for doctors,

nurses and psychologists, except for so-called plus doctors and emergency services. The

narrow authority is said to mean that users can only take part

information about patients (both internal medical records and NPÖ) at patient meetings.

It is further stated that access is granted in connection with the staff

scheduled with patient and automatically withdrawn 4 months after

access granted and that before meeting with patient has taken place can not

beating on such patient happen.

The Data Inspectorate states that KRY since the inspection on April 4, 2019

has improved its needs and risk analysis so that it increasingly

meets the requirements for a needs and risk analysis. The Data Inspectorate

notes, however, that the analysis does not describe the risks for those registered on other than that it is stated that there is a risk of disclosure of confidentiality and privacy damage or privacy threat. The analysis lacks a more detailed description of what such injury or threat consists of and the extent of the treatment affects the risk.

The Data Inspectorate therefore submits KRY, pursuant to Article 58 (2) (d) i the Data Protection Regulation, to be completed by the last February 2021 at the latest the needs and risk analyzes for the journal systems ProReNata and Nationell patient overview by developing the analysis of the risks for those registered rights and freedoms and that thereafter, with the support of needs and the risk analyzes, make a reassessment regarding the allocation of permissions so that each user has access to only those personal data needed for the user to be able to fulfill his duties in health care, in accordance with Article 32 (1) and

32.2 of the Data Protection Ordinance, Chapter 4 § 2 and ch. 6 Section 7 of the Patient Data Act and Chapter 4 2 § HSLF-FS 2016: 40.

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 Hans-Olof Lindblom, General Counsel

unit managers Malin Blixt and Katarina Tullstedt participated.

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

Appendix: Appendix 1 - How to pay a penalty fee

Copy for information to:

Data Protection Officer

How to appeal

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

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

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

the day you received the decision. 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.