Decision

Diary no

2020-12-02

DI-2019-3845

Digital Medical Supply Sweden AB (KRY)

Torsgatan 21

113 21 Stockholm

Supervision according to the data protection regulation and

the patient data act – needs and risk analysis and

questions about access in the record system to Digital

Medical Supply Sweden AB (KRY)

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

Content

The Swedish Data Protection Authority's decision..... 3

Statement of the supervisory case..... 4

What emerged in the case..... 5

Personal data controller..... 5

Operation..... 5

Journal system..... 5

Users and patients..... 5

Internal confidentiality..... 6

Needs and risk analysis..... 6

Authorization assignment for access to personal data..... 9

Coherent record keeping..... 10

Needs and risk analysis..... 10

Authorization assignment regarding access to personal data about

patients..... 10

Documentation of the access (logs)..... 11

Justification of the decision..... 12

Applicable rules..... 12

The Data Protection Ordinance the primary source of law..... 12

The Data Protection Regulation and the relationship with supplementary national

regulations..... 13

Complementary national provisions..... .. 14

Requirement to carry out a needs and risk analysis..... 15

Internal confidentiality..... 16

Coherent record keeping..... 16

Documentation of access (logs)..... 17

The Swedish Data Protection Authority's assessment..... 17

Personal data controller's responsibility for security..... 17

Needs and risk analysis..... 18

Authorization assignment for access to personal data about patients... 23

Documentation of the 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 Swedish Data Protection Authority's decision

During an on-site inspection on April 4, 2019, the Norwegian Data Protection Authority found that

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

with article 5.1 f and 5.2 and article 32.1 0ch 32.2 of the data protection regulation1

by

1.

KRY has not carried out needs and risk analyzes that fulfill

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

the patient data act (2008:355) and ch. 4 § 2 of the National Board of Health and Welfare

regulations and general advice on record keeping and treatment of

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

assignment of authorizations takes place in the journal system ProReNata and

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

extent has taken appropriate organizational measures to

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

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

the risks.

2. KRY has not shown that KRY limited the user's permissions too

access to the record system ProReNata and National patient overview

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

fulfill their duties in health and medical care in accordance

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

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

sufficient measures

measures to be able to ensure and be able to demonstrate appropriate security

for the personal data.

The Swedish Data Protection Authority states that KRY since the inspection on 4 April 2019

have improved their needs and risk analyses, but that the analyzes not in all

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

the patient data act (2008:355) and ch. 4 § 2 The National Board of Health and Welfare's regulations and

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

Datainspektionen orders with the support of article 58.2 d i

data protection regulation KRY to be supplemented by the end of February 2021 at the latest

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

patient overview by developing the analysis of the risks for the registrants

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

the risk analyses, make a renewed assessment regarding the allocation of

permissions so that each user can access only them

personal data that is needed for the user to be able to fulfill their

tasks within the health and medical care, in accordance with article 32.1 and

32.2 of the data protection regulation, ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and

4 ch. Section 2 HSLF-FS 2016:40.

Account of the supervisory matter

The Swedish Data Protection Authority initiated supervision by means of a letter on 22 March 2019 and

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

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

covered how KRY assigned permissions for access to

the main record system ProReNata and National patient overview and which

access opportunities the assigned permissions provide within the scope of as well as

the internal secrecy according to ch. 4 the Patient Data Act, as the consolidated

record keeping according to ch. 6 the patient data act. In addition to this have

The Swedish Data Protection Authority also reviewed the documentation of access (logs)

which is in the journal system.

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

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

part of and read. The supervision does not include which functions are included in

the authorization, i.e. what the user can actually do in the records system

(e.g. issuing prescriptions, writing referrals, etc.).

What emerged in the case

KRY has essentially stated the following.

Personal data controller

KRY is a healthcare provider and personal data controller.

Operation

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

It is KRY's parent company Webhälsa AB (hereinafter Webhälsa) that has developed the app and manages the operation of the technical platform. Webbhälsa owns the KRY brand, develops the technology and serves the healthcare provider KRY with licenses. There are two separate legal entities 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, Webbhälsa turned to regions and county council to offer the service, but it took a long time to get care providers to start using the service. That's why Webbhälsa started the company KRY as one own care provider who provides care via the KRY app.

Journal system

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

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 registered in ProReNata 450 331.

Internal confidentiality

Needs and risk analysis

During the inspection and subsequent review, mainly the following

arrived.

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

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

revised needs and risk analysis dated 2 May 2019 there also consolidated

record keeping is included but otherwise essentially contains the same needs and risk analysis as the document dated March

11, 2019. March 20, 2020

received KRY with a new revised version dated 1 March 2020 which contains

a largely revised analysis.

The needs and risk analysis dated 11 March 2019 includes, among other things, a

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

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

healthcare professionals:

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

presence in different geographical areas, healthcare staff at KRY are organized in

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

patients. Health care professionals are thus not organized exclusively based on

necessary competence in the individual case (e.g. general practitioner, nurse or psychologist),

scheduling and availability. Although certain types of treatment, e.g. treatment of children

under 6 months of age or treatment of certain symptoms typical of e.g. women, must be taken care of

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

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

through e.g. a larger number of available employees, several different categories of care staff or

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

carried out to ensure patient safety but also ensure that respect for the patient's

integrity is constantly observed.

In order to ensure good quality, availability and cost-effectiveness, it is of utmost importance to 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 clinicians and relevant administrative staff (such as medical secretaries who have relevant training for their mission) who are 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 to be able to fulfill their duties.

In summary, it is KRY's assessment that due to both the nature and uniqueness of the business characteristic there is a great need not to limit eligibility for medical and relevant administrative staff to certain geographically or demographically defined patient groups i the current situation. For other types of permissions, 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 authority and indicates that the risks in KRY's opinion are mainly:

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

- Unauthorized access for healthcare professionals or relevant administrative staff as a result of willful abuse;
- Unauthorized access by third parties as a result of health and healthcare staff or relevant administrative staff lose equipment or, knowingly or unknowingly, share system login details; and
- Unauthorized access by third parties as a result of data breaches.

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

- Procedures for recruitment, 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 tutoring and training around the use of systems, equipment, relevant constitutions and routines regarding confidentiality and patient safety in order to raise awareness of duties, rights and responsibilities;
- Signing a reminder of confidentiality and/or confidentiality commitments for to proactively reduce the risk of unauthorized access and to increase

the knowledge of confidentiality and patient safety;

Use of equipment provided and controlled by

CRY;

Procedures for assigning, changing and removing authorizations for

to preventively minimize the risk that authorizations are not adequate

over time;

Technical tools to preventively minimize the need for beatings i

the records system and thus the risk of unauthorized access, e.g. like one

result of mistakes or insufficient knowledge. In health and

healthcare staff's work for digital care, will only be relevant

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

as the meeting relates to opening. To be able to search for other patients

must current staff actively make an illegal hit;

Obtaining consent from patient before medical

secretaries make punches in patient records; and

Clear information to relevant personnel and routine for logging and

control with the aim of preventively getting employees to refrain from unauthorized

access and to reactively detect and follow up on such

access. All journal entries that are not linked to one

active care relationship/performed patient meeting is logged and reviewed

manually.

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

A broad authorization for medical and administrative staff to patients

records is 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 re-examined regularly and may be

changes as KRY grows, changes medical direction, develops

its business concept and in other similar circumstances. One

prerequisite 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 one significantly

larger workforce than the one currently available for KRY, but is one

desirable goal to aim for in the long term.

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

the analysis and identified risks based on certain types of information and

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

public figures, employees and the staff's own data. Furthermore, have

KRY in the revised analysis also assessed probability and consequence for

the identified risks. The analysis also contains more detailed

review of access needs for the various staff categories. To

different from the previous versions of the analysis KRY has arrived at

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

except so-called plus doctors, plus psychologists and back-up doctors. The narrow one

the authorization is said to mean that users can only access data

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

stated that access is granted in conjunction with the staff being scheduled with

patient and is automatically withdrawn 4 months after access is granted

and that before the meeting with the patient has taken place, such patient cannot be beaten

happen.

Authorization assignment for access to personal data

During the inspection, the following mainly emerged.

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

psychologists as well as 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 in the assessment of authorization management there

KRY thought about what other security could be offered.

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

is matched against whether clinicians had an appointment with the patient that day. In other

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

explanation of the access. There is a check every four weeks when applicable

active accounts (by going through the personnel schedule). If, for example, a

doctors who do not have a pass booked in the next four weeks will be deactivated

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

in the next four weeks, the account will be activated.

The design of the authorizations is based on the digital nature of

the service that KRY offers, that the care has a general focus and is not

specialized, that the patients are spread all over the country, that the waiting 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 is helped by 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 the doctors must be able to see each other

medical records to be able to provide good care.

KRY has made the assessment that all information available about the patients is

relevant for the healthcare staff, but KRY is aware that this may come

to change as the organization grows.

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

detailed analysis of the need for access to data in ProReNata based on those

the tasks of the different staff categories and arrived at a narrow

authorization is sufficient for doctors, nurses and psychologists in that way

as described in the section above in the statement of the revised needs and

the risk analysis.

Coherent record keeping

During the inspection and subsequent review, mainly the following

arrived.

Needs and risk analysis

At the time of the inspection, there was no special needs and risk analysis for access to

NPÖ. KRY has submitted two revised needs and risk analyses

dated 2 May 2019 and 1 March 2020 covering the use of national patient overview (NPÖ) in the business. The needs and risk analysis dated 2 May 2019 otherwise essentially contains 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 made one more detailed analysis of the need for access to data in NPÖ based on the different the tasks of the personnel categories.

Authorization assignment regarding access to personal data about patients

KRY has stated that the care provider is part of the system for cohesion record keeping through NPÖ as a "consumer". This means that the staff at KRY can access the data in NPÖ, but KRY "produces" (makes available) no own data in NPÖ.

At the time of the inspection it was found that all personnel who had access to ProReNata also had access to NPÖ.

From the revised needs and risk analysis dated March 1, 2020, it appears that all staff 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 the access (logs)

KRY has stated the following.

For each stroke in ProReNata, a log message with information is created about which personnel made a strike at a given time. Time

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

the user's identity, what action the user has taken, for example

signing, noting and reading. Because KRY are 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. Visit log shows when a user visited a journal and

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

server calls to a journal and may imply that users have read but also

other reasons. Event log displays logged system events that affect a

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

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

CRY.

KRY has noted after the inspection that the specific measure

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

KRY has taken this up with ProReNata AB who, at KRY's request, have

developed such logging. Even cancellations of notes will come

therefore 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 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.

From article 5.2 it appears that the so-called the liability, i.e. that it

personal data controller must be responsible for and be able to demonstrate that the basic

the principles in point 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).

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 in the processing of 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, i.e.
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.

According to ch. 4 § 2 HSLF-FS 2016:40, 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

The 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 § 2 also

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

that 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 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.

The security in connection 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 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 to 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 written, 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 and the data concerned
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 everyone and
the data may over time be processed by many people.
All in all, this places great demands on the person in charge of personal data.

The data that is processed must be protected against external actors as well
the business as against unauthorized access from within the business. It can
it is noted that in article 32.2 it is stated that the person in charge of personal data, at
assessment of the appropriate security level, in particular must take into account the risks of
accidental or unlawful destruction, loss or unauthorized disclosure or
unauthorized access. In order to know what is an unauthorized access must
the personal data controller is clear about what constitutes an authorized access.

Needs and risk analysis

In the National Board of Health and Welfare's regulations that supplement the Patient Data Act, there is
stated in ch. 4 § 2 HSLF-FS 2016:40, 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 personal data
about patients. Both the needs and the risks must be assessed based on them

information that needs to be processed in the business, what processes it is
the question of whether and what risks exist for the individual's privacy.

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

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

authorization levels must exist (prop. 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 shall

be kept up to date.

In summary, the regulation requires that the risk analysis identify

-

different categories of data,

-

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 based on
the nature, scope, context and purpose of the processing (reason 76).

It is thus through the needs and risk analysis that it
data controller finds out who needs access, which
data the access must cover, 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 there is no access other 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 during the inspection requested a documented
needs and risk analysis was submitted to KRY with a document dated 11 March 2019

with the heading "Authority allocation Needs and risk analysis". KRY has
then on 10 May 2019 KRY received a revised needs and
risk analysis dated 2 May 2019, which also includes coherent record keeping
but which otherwise essentially contains the same needs and risk analysis as
the document dated March 11, 2019. On March 20, 2020, KRY received a new
revised version dated March 1, 2020 which contains a large part
revised analysis.

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

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

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

to reduce the risk of unauthorized access.

On the other hand, KRY has not taken into account how negative in its initial analysis 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 is also a lack of special risk assessments based on whether there is e.g. protected personal data marked confidential, information about general famous people, information from certain receptions or medical specialties or other factors that require special protective measures. The there is also an assessment of how likely and serious the risk is for them data subject's rights and freedoms are deemed to be.

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

In summary, the Data Inspectorate notes that KRY at the inspection occasion carried out a needs and risk analysis at a strategic level, but that it has not met the requirements the data protection regulations place on one such analysis because KRY has not considered the risks, of varying degree of probability and seriousness, for the rights and freedoms of natural persons and did not take into account various risks to the individual's integrity that may be associated with too wide availability regarding certain types of information.

The Norwegian Data Inspection Authority states that KRY thereby at the time of the inspection

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

is set in

4 ch. § 2 HSLF-FS 2016:40, whether within the framework of internal confidentiality

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

6 ch. the patient data act. This means that KRY has not taken the appropriate measures

organizational measures in accordance with article 5.1 f and article 31.1 and 31.2 for

to be able to ensure and, in accordance with Article 5.2, to be able to demonstrate that

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

the analysis and identified risks based on certain types of information and

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

public figures, employees and the staff's own information. Furthermore, have

KRY in the revised analysis also assessed probability and consequence for

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 forward

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

except so-called plus doctors, plus psychologists and back-up doctors. The narrow one

the authorization is said to mean that users can only access data

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

stated that access is granted in conjunction with the staff being scheduled with

patient and is automatically withdrawn 4 months after access is granted

and that before the meeting with the patient has taken place, such patient cannot be beaten

happen.

The Swedish Data Protection Authority 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 takes into account different things in each case

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

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

based on the new roles created more limited access possibilities.

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

further assessments are required regarding the needs. As far as the risks are concerned

they are still not analyzed based on categories of data. Tasks

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

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

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

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

undergo. 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

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

of access.

Permission assignment for 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, i.a. that there must be different authorization categories in the journal system and that the authorizations must be limited to what the user need to provide the patient with good and safe care. It also appears that "one more expansive or coarse-grained authority assignment should be considered a unjustified dissemination of medical records within a business and should as such is not accepted."

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.

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

of healthcare professionals and medical secretaries

access possibilities to information about patients either within the framework of it

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

coherent record keeping in the NPÖ record system. 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 as well as deactivation

of accounts every four weeks for doctors without a passport booked in the next four

the weeks.

Because the needs and risk analysis that KRY had carried out at

the timing of the inspection was not sufficiently taken into account

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

risks that may be associated with an excessively wide availability regard

certain types of data, KRY has not shown that the read permissions have been restricted

in the manner required by the Data Protection Regulation 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

confidentiality, partly within the framework of coherent record keeping. CRY

has subsequently reduced that risk through improved measures

analyzes and subsequent measures taken.

Against the background of the above, the Data Inspectorate can state that KRY at

the inspection occasion has processed personal data in violation of Article 5.1 f

and Article 32.1 0ch 32.2 of the data protection regulation by KRY, in accordance

with article 5.2 and 24.1, has not been able to show that KRY limited the users'
authorizations for access to the records system ProReNata and National
patient overview to what is only needed for the user to be able to
fulfill their duties within health care according to ch. 4 § 2 and
6 ch. Section 7 of the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40.
In the needs and risk analysis dated March 1, 2020, it appears that KRY has introduced
restrictions on access to personal data about patients. Unlike
the previous versions of the analysis, KRY has concluded that a narrow
authorization is sufficient for doctors, nurses and psychologists, except so-called
plus doctors, plus psychologists and doctors on call. The narrow authorization
is said 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 conjunction with the staff is scheduled with the patient and drawn
automatically back 4 months after access is granted and before
meeting with a patient has taken place, hitting such a patient cannot take place.
KRY has thus improved the restriction of access since the inspection.
According to what appears in the section above regarding the new needs and
However, the risk analysis still requires some additions to the analysis
must be comprehensive and able to demonstrate that access has been restricted accordingly
with the requirements of the Data Protection Regulation and the Patient Data Act. From
the result of these additions must then KRY assess its model for
authorization assignment.
Documentation of the access (logs)

The Swedish Data Protection Authority can state that from the logs in ProReNata and NPÖ

information about which staff at a given time made a

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

patient concerned, the identity of the user, what the user has taken for

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

organized in several different care units, only one unit appears which is

the same for all staff.

KRY has noted after the inspection that the specific measure

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

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

May 2019. The Swedish Data Protection Authority states that the documentation of the access

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

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

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

pursuant to 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. 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 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.
Assessment of whether a penalty fee should be imposed
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 written, 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.
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 assignment that is even more
finely divided. It is therefore essential that there is a real analysis of the needs
based on different businesses and different executives. Equally important is that
there is an actual analysis of the risks based on an integrity perspective

can occur in the event of an excessive assignment of authorization to access. From

access to this analysis must then be limited to the individual executive.

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

hand that changes in the individual executive's duties provide

reason for it.

The Swedish Data Protection Authority has established that KRY during the Data Protection Authority's inspection

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

not fully considered the risks, of varying degrees of probability and seriousness, for

rights and freedoms of natural persons and that KRY has not considered different

kind of risks to the individual's integrity that may be associated with a

too in case of availability regarding certain types of information. KRY has subsequently i

March 2020 carried out a new needs and risk analysis. The new needs and

the risk analysis goes deeper than the previous one and considers both organization and

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

deepened and now also includes an assessment of probability and

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

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

still parts relating to the risk assessment. What closer needs

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

The Danish Data Protection Authority's supervision has thus shown that KRY has not met the requirement for

to take appropriate security measures to provide protection to the personal data i

the records systems by not having fully lived up to the requirements that follow

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

before assigning 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

nor has met the requirements in Article 5.1 f and Article 32.1 and 32.2 i

data protection regulation. The lack of regulatory compliance includes both

the internal secrecy according to ch. 4 the Patient Data Act as the consolidated

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

The Data Inspectorate can state that the violations as a starting point are

serious as it concerns provisions that are fundamental to ensure that

the processing of personal data is subject to sufficient security measures

for the protection of data subjects' basic 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, such as the number of employees and access for a large part of them

employees to these patients' tasks speak in an aggravating direction.

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.

It is thus typically not a question of minor violations but

violations that should normally lead to an administrative penalty fee.

When assessing whether a penalty fee should be imposed, it must be tested at the same time

if required in view of the fact that it is to be a measure as in that

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 likely

reduces the risk to the rights and freedoms of natural persons. KRY thus has

tried to comply with the requirements set for the processing of personal data and has

to a not inconsiderable extent taken measures with the aim of complying with the requirements and

reduce the risks. The Swedish Data Protection Authority assesses that KRY's lack of compliance

has not meant that the registered have been deprived of protection for 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

deficiencies in the needs and risk analysis after the Data Inspectorate's inspection through

to draw up and submit to the Data Inspectorate with two revised needs and risk analyses. It should also be taken into account

that KRY itself has drawn attention

deficiency in logging and has taken steps to remedy that deficiency.

In a balanced assessment, the Swedish Data Protection Authority finds that the relevant

the violations are admittedly typically of such a nature that a

administrative penalty fee should normally be imposed but that in the current case

the case is not proportionate to such an intervention from

The Swedish Data Protection Authority. KRY should instead be instructed 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 takes into account the revisions of

the needs and risk analysis that KRY has done after the inspection.

KRY has revised its needs and

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

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

KRY adjusted the analysis to also include coherent record keeping i

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 information about persons with protected identity, public figures,

employees and the staff's own tasks.

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

consequence for the identified risks. The analysis also contains more

detailed review of access needs for the various

the personnel categories. Unlike the previous versions of the analysis

has KRY concluded that a narrow qualification is sufficient for doctors,

nurses and psychologists, except so-called plus doctors and back-up doctors. The

the narrow authorization is said to mean that users can only take part in

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

Furthermore, it is stated that access is granted in connection with the staff

scheduled with patient and automatically withdrawn 4 months after that

access has been granted and that before the meeting with the patient has taken place cannot

beating on such patient take place.

The Swedish Data Protection Authority states that KRY since the inspection on 4 April 2019

has improved its needs and risk analysis so that it increasingly

meets the requirements set for a needs and risk analysis. The Swedish Data Protection Authority

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

The Swedish Data Protection Authority therefore instructs KRY, with the support of Article 58.2 d i
data protection regulation, to supplement by the end of February 2021 at the latest
the needs and risk analyzes for the record systems ProReNata and Nationell
patient overview by developing the analysis of the risks for the registrants
rights and freedoms and that thereafter, with the support of needs and
the risk analyses, make a renewed assessment regarding the allocation of
permissions so that each user can access only them
personal data that is needed for the user to be able to fulfill their
tasks within the health and medical care, in accordance with article 32.1 and

32.2 of the data protection regulation, ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and
4 ch. Section 2 HSLF-FS 2016:40.

This decision has been made by the director general Lena Lindgren Schelin after
presentation by IT security specialist Magnus Bergström. At the final
the handling is also handled by chief legal officer Hans-Olof Lindblom as well

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 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 Data Protection Authority no later than three weeks from the day you were informed of the decision. 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.