Decision

Diarienr

2020-12-02

DI-2019-3841

The Health and Medical Care Board at

Västerbotten Region

Köksvägen 11

901 89 Umeå

Supervision under the Data Protection Regulation and

Patient Data Act - needs and risk analysis

and questions about access in journal systems

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

The Data Inspectorate's decision

The Data Inspectorate has at the inspection on 14 May 2019 and 12 December 2019 established that the Health and Medical Care Board at Region Västerbotten processes personal data in breach of Article 5 (1) (f) and (2) and Article 32 (1) 0ch 32.2 of the Data Protection Regulation1 by

1.

The Health and Medical Care Board has not implemented needs and

risk analysis before the allocation of authorizations takes place in the record system

NCS Cross, in accordance with ch. § 2 and ch. 6 Section 7 of the Patient Data Act

(2008: 355) and ch. 4 Section 2 The National Board of Health and Welfare's regulations and general

advice (HSLF-FS 2016: 40) on record keeping and treatment of

personal data in health care. This means that Health and

the health care board has not 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. The Health and Medical Care Board has not restricted users

permissions for access to the NCS Cross journal system to what

only needed for the user to be able to fulfill theirs

tasks in health care in accordance with

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

2016: 40. This means that the Health and Medical Care Board does not have

taken measures to be able to ensure and be able to show a suitable

security of personal data.

The Data Inspectorate decides on the basis of Articles 58 (2) and 83 i

the Data Protection Ordinance and Chapter 6 § 2 of the law (2018: 218) with

supplementary provisions to the EU Data Protection Regulation that the Health and Medical Care Board, for the violations of

Article 5 (1) (f) and (2) and

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

administrative penalty fee of 2,500,000 (two million

five hundred thousand) kronor.

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

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

Data Protection Ordinance The Health Care Board to implement and

document the required needs and risk analysis for the NCS medical record system

Cross and then, with the support of the needs and risk analysis, assign each

user individual authorization for access to personal data to only

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

in the field of health, in accordance with Article 5 (1) (f) and Article 32 (1) and

32.2 of the Data Protection Ordinance, Chapter 4 § 2 and ch. 6 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 14 May 2019 and 12 December 2019 reviewed whether the Health and Medical Care Board's decision on the

allocation of qualifications has been preceded

of a needs and risk analysis. The review has also included how the Health and Medical Care Board has granted authorizations

for access to

the main journal system NCS Cross, and what access possibilities they were allocated

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

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

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

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

The Data Inspectorate has only examined the user's access options to

the journal system, 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.).

Previous review of needs and risk analyzes

The Data Inspectorate has previously carried out an inspection regarding the then

The County Council Board, Västerbotten County Council had implemented one

documented needs and risk analysis according to ch. § 6 second paragraph second

the sentence of the National Board of Health and Welfare's regulations (SOSFS 2008: 14) on

information management and record keeping in health care. Of

The Data Inspectorate's decision with registration number 1615-2013, announced on 27

March 2015, it appears that the County Council Board did not meet the requirement that

carry out a needs and risk analysis in accordance with the said regulations, and

was therefore instructed to implement one for the main record system.

What has emerged in the case

The Health and Medical Care Board has mainly stated the following.

Personal data manager

On January 1, 2019, a reorganization was made which meant that Region

Västerbotten was formed. There is no authority under Health and

the health care board. The Health and Medical Care Board conducts health and

healthcare within the region and is responsible for the processing of personal data

personal data that the business performs in the main record system NCS Cross.

Journal system

The main journal system used is called NCS Cross and stands for Nordic Clinical Suite. It is possible to take part in care documentation in NCS Cross from 1993 when the system was introduced. At that time was the allocation of privileges was more limited and users had access to fewer data than in the current system. The so-called Employee Assignments was added in 2014–2015. Employee assignments regulate on which organizational level access can be done in NCS Cross and is required to access the system.

NCS Cross is used within the framework of coherent record keeping together with seven other care providers.

In connection with the Data Protection Ordinance began to apply the supplier a general review of the system and informed that no functional adjustments needed to be made.

There are 101 databases in NCS Cross based on the fact that each clinic basically has one own database. Within the Västerbotten Region, the number of units is 84 (active databases). Within NCS Cross, there are so-called protected units.

In NCS Cross, it is possible to control the staff's access possibilities different ways in terms of authorization management, including through employee assignments and functions for blocking records.

Protected information, about patients with a protected identity at the Swedish Tax Agency, is not available in NCS Cross.

The number of patients and employees

The number of unique registered patients in NCS Cross within the framework of the internal

confidentiality is 652,995. The number of patients registered within the framework

for unified record keeping is 665,564.

There are approximately 10,000 employees in the Västerbotten Region. Within the region

9,139 users have a valid employee assignment and active account in NCS

Cross. The number of active user accounts in the region is 12,366. The reason

to the difference in the number of users is that the businesses have not reported

to the administration that the authorization is to be terminated. Access to NCS Cross

stopped anyway because the users who do not have an employee assignment

can not log in to the application. The process is automated so that the AD account and thus also the employee assignment is

closed automatically when

the employment ends.

Internal secrecy

Needs and risk analysis

The Data Inspectorate's decision of 27 March 2015 states that

The County Council Board, Västerbotten County Council, was instructed to produce one

documented needs and risk analysis for the main record system.

Against this background, the Health and Medical Care Board has stated, among other things

following.

The Health and Medical Care Board has followed the Data Inspectorate's previous decisions

and produced the documents Guideline for information security and

management and operation and Template - Needs and risk analysis at

authorization. The control document and template have been created to provide

the business managers tools in connection with the allocation of authority.

The documents User profiles are examples that clarify that permissions

not assigned generally but individually. The documents are also examples of

performed analyzes at actual eligibility assignments within various

units.2 The needs and risk analysis is made from the business perspective and

not from an integrity perspective.

2

The documents have been received by the Data Inspectorate.

The committee does not know to what extent the template Template - Needs and risk analysis

when allocating permissions is used in the business, when you only see

the result of the authorization order itself. The board has assumed that

the business managers make a needs and risk analysis before ordering

permissions. However, the committee has not seen any documented needs and

risk analysis neither for internal secrecy nor for cohesion

record keeping.

The guidelines for information security state that authorization must be granted

after an analysis of what information different staff categories in different

businesses need. The guidelines also state that the risk analysis must take place

consideration of the risks it may entail if the staff has too little or too little

much access to various patient data. Then the needs vary between different

types of activities, the business manager is responsible for the needs and

risk analysis is carried out at unit level. According to the guidelines, the business should

document the needs and risk analysis when allocating

the employee assignment.

The guidelines also state, among other things, that in addition to regular inspections of the users' authorization needs, the authorizations must be reviewed accordingly organizational and system change.

Authorization of access to personal data about patients

The Health and Medical Care Board has mainly stated the following.

In order for an executive to be able to access personal data in NCS Cross several conditions need to be met. The executive must have one active user account in the region domain (AD). This in turn presupposes that the executive is registered in the HR system. To be able to log in to domain, executives need a SITHS card with one or more valid ones certificate. To then be able to log in to NCS Cross needs the executive partly have a valid so-called employee assignment, partly become assigned a license in NCS Cross. The employee assignment regulates on which organizational level access can be done in NCS Cross. It is the heads of operations of the various units that decide on the allocation of the employee assignment to his staff at the care unit.

Two-step authentication "that you really are who you are" and that access closes to the user when he quits are examples of actual actions such as taken to prevent unnecessary dissemination of personal data.

The qualifications assigned to the staff are based on the needs analysis that is performed before the assignment, ie where and with what the employee works.

For example, counselors and physiotherapists may be employed in different units,

which means that they have more employee assignments and thus must be given access to more devices. The same applies to emergency physicians who also have access to more units than the own emergency database.

The staff's access to databases is based on the need that exists. One employee assignments can thus mean that an employee can be authorized to multiple databases. A nurse at Neurocentrum can, for example, get one employee assignments with access to eight databases because the clinic has eight databases and the nurse's work requires access to all of them.

Access opportunities (read access) to care documentation in NCS Cross

Each employee has a reading authority that is adapted based on the individual's mission. If an employee is assigned reading permission within the entire Region Västerbotten only applies to care documentation. Protected devices are excluded.

In the NCS Cross authorization control system, there are two types of authorizations Own competence, partly Service role.

Own authority means that an executive is given access to them functions in the record system that are relevant to the executive tasks, such as prescribing medicines. Own authority also means that the executive is given permission to read and write to them parts of the journal system (databases) that are linked to it or they care units where the executive is active.

Eligibility according to the position role means that an executive is also given read access to other databases in the journal system. The executive can then the service role is given Reading permission VLL, which means access (read access) to all units' care documentation in the Region Västerbotten, except for protected units. Executives can be assigned one

other reading permission than Reading permission VLL. Read access to

personal data of protected entities are provided only within the framework of the allocation of

Own authority.

The module that handles the journal in NCS Cross is heading

Care documentation. The module contains all documentation that is available

the patient in accordance with ch. 4 § 1 Patient Data Act. There are others as well

modules, such as Care Administration, which contain information in accordance

with ch. 2 4 § 2 of the Patient Data Act.

Doctors are almost always assigned a Reading Permit VLL. Regarding

the nurses are often ordered to read VLL, which means that a

majority of nurses are assigned this reading privilege. Have the staff

assigned write permission in the system, it means that the staff also has

readability in it. The number of executives who have Reading Authorization VLL in

NCS Cross has a total of 7,586. Of these, 2,290 are doctors, 3,759 are nurses,

124 are assistant nurses including pediatric nurses and 956 are paramedics.

The information is valid for December 2019.

Restrictions on access to data in NCS Cross

There are no direct barriers to introducing restrictive features

read access and thus access in NCS Cross. The system enables

assigning permissions that give users different access options.

It can be done at the individual level. You can also restrict access to some

devices. Technically, for example, it is possible to exclude BUP from

access possibilities. Operations managers can restrict access and control privileges so that the staff of a unit has access to data only about care and treatment at the relevant unit and not such information at others devices.

NCS Cross 84 units have the following six protected units. 1) The device clinical genetics, 2) Unit for Child and Adolescent Habilitation 3) Section child and adolescent habilitation within the unit child and adolescent clinic Västerbotten 4) Section for children's homes, within the unit for children and youth psychiatry Västerbotten 5) Occupational health care 6) The LSS units in disability activities, visual and hearing rehabilitation and support and habilitation for adults and the section on the exercise of authority in the Support Unit and habilitation for adults.

An active choice for access is required by the user when the patient has blocked his care documentation.

Coherent record keeping

The Health and Medical Care Board has mainly stated the following.

Needs and risk analysis

Template Template - Needs and risk analysis when allocating eligibility also applies for the unified record keeping. Needs analysis done before authorization allocation also includes analysis for access within the framework of coherent record keeping.

Authorization of access to personal data about patients

If an employee has been granted reading authority in the internal secrecy, it means

that he has also been granted reading permission for the unified record keeping.

Access opportunities (read access) to care documentation in NCS Cross

The reading authority within the coherent record keeping is the same as

for internal secrecy. This means that the staff can take part in everything

care documentation about all patients who are in the system for it

coherent record keeping. The basis for this lies

employee assignment.

Restrictions on access to data in NCS Cross

Employees must make active choices to access information in it

keep the record keeping together, ie answer the question of whether the patient has given

their consent or state that there is an emergency in order to be able to take part

of the data.

Documentation of access (logs)

The Health and Medical Care Board has stated, among other things, the following.

Each time a user enters NCS Cross, the activity is logged. The search on

a patient can be made on social security number or backup number. According to

guidelines, the system should once a month select ten users on one

unit. In such a log check, all patient records are displayed as respective

users opened for login during the checked log period as well

all activities done in the care portal: time, activity, social security number,

patient, journal, information, staff, title, location, client, purpose

and date.

In the log extract, it is stated under the heading Client at which unit

the measures have been taken, ie which care unit's employee assignment

the user used at login. Under the heading Journal it is stated

database from which the staff retrieved data, ie at which

care unit documentation the user reads in.

The database called Medicincentrum contains care documentation from two

care units, partly Medicincentrum, partly Hjärtcentrum. If, for example

login is done in the database Medicincentrum by a doctor who works at

the unit Medicincentrum, the log extract will state Medicincentrum

both under the heading Client and the heading Journal. About the doctor

on the other hand, working at Hjärtcentrum is included in the log extract under the heading

Client to be specified Heart Center.

The log entries generated refer to both the internal confidentiality and the

coherent record keeping.

The Health and Medical Care Board has submitted to the Swedish Data Inspectorate

log extract with documentation of the accesses (logs) that were created with

due to the inspection of the inspection.

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, the personal data shall

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 under Article 6 (1). c and the exercise of authority in accordance with 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 exemption in Article 9 (2). h need
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 as to how

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

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

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

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

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

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

personal data in health care.

National provisions that supplement the requirements of the Data Protection Regulation

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

2016: 40.

Requirement to do needs and risk analysis

The care provider must, according to ch. § 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 data shall

limited to what the executive needs to be able to perform his

tasks in health care. This includes that permissions should

followed up and changed or reduced over time as changes in the individual

the executive's duties 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 of the responsible caregiver to make active and

individual eligibility assignments based on analyzes of which details

information different staff categories and different types of activities need. But

not only needs analyzes are needed. Risk analyzes must also be done where you take them

account of various kinds of risks that may be associated with an overly wide

availability of certain types of data. Protected personal data that is

classified, information on public figures, information from certain

receptions or medical specialties are examples of categories that can

require special risk assessments.

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

there must be a greater variety of eligibility levels. Decisive for decision on

eligibility for e.g. different categories of health care professionals to

electronic access to information in patient records should be that the authorization should

limited to what the executive needs for the purpose a good and safe

patient care. A more extensive or coarse-grained grant should -

even if it would have points from an efficiency point of view - considered as one

unjustified dissemination of journal information within a business and should as such

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

tasks. In the case of staff working with business follow-up,

statistical production, central financial administration and similar activities

which is not individual-oriented, this should be sufficient for most executives

access to data that can only be indirectly derived from individual patients.

Electronic access to code keys, social security numbers and other information such as

directly pointing out individual patients should be able to 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, that the care provider shall 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 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, thus 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 Article 32 of the Data Protection Regulation.

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

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

The health service has a great need for information in its operations. The It is therefore natural that the possibilities of digitalisation are utilized as much as possible in healthcare. Since the Patient Data Act was introduced, a lot

extensive digitization has taken place in healthcare. Both the data collections

size as the number of people sharing information with each other has increased

substantially. At the same time, this increase means that the demands on it increase

personal data controller, as the assessment of what is an appropriate

safety is affected by the extent of the treatment.

It is also a question of sensitive personal data. The information concerns

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

It is also often a question of a lot of personal information about each of these

people and the data may over time may be processed by very

many people in healthcare. All in all, this places great demands on it

personal data controller.

The data processed must be protected from outside actors as well

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

of Article 32 (2) that the data controller, in assessing the appropriate

level of security, in particular to take into account the risks of unintentional or illegal

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

be able to know what is an unauthorized access it must

personal data controllers must be clear about what an authorized access is.

Needs and risk analysis

I 4 kap. Section 2 of the National Board of Health and Welfare's regulations (HSLF-FS 2016: 40), which supplement

In the Patient Data Act, it is stated that the care provider must make a needs and

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

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

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

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

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

with an overly allotment of access to personal data

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

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

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

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

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

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

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

that it is a question of protected personal data or data of general

famous people. The size of the system also affects the risk assessment. Of

The preparatory work for the Patient Data Act states that the more comprehensive one

information system is, the greater the variety of authorization levels required

there is. (Prop. 2007/08: 126 p. 149).

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

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

updated.

In summary, the regulation requires that the risk analysis identify

- different categories of data (eg health data),
- categories of data subjects (eg vulnerable natural persons and

children), or

- the scope (eg number of personal data and registered)
- negative consequences for data subjects (eg damages,
significant social or economic disadvantage, deprivation of rights
and freedoms),
and how they affect the risk to the rights and freedoms of natural persons
Processing of personal data. This applies to both internal secrecy
as in coherent record keeping.

The risk analysis must also include special risk assessments, for example
based on whether there is protected personal data that is
classified, information on public figures, information from
certain clinics or medical specialties (Bill 2007/08: 126 p. 148149).

The risk analysis must also include an assessment of how probable and serious
the risk to the data subjects' rights and freedoms is and in any case determined
whether it is a risk or a high risk (recital 76).

It is thus through the needs and risk analysis that it
personal data controller finds out who needs access, which

information the accessibility shall include, at what times and at what
context access is needed, while analyzing the risks to it
the freedoms and rights of the individual that the treatment may lead to. The result should
then lead to the technical and organizational measures needed to

ensure that no access other than that of need and

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

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

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

be able to assign their users a correct authorization. The

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

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

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

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

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

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

required.

The Health and Medical Care Board's work with needs and risk analysis

When the Data Inspectorate has requested a documented needs and

risk analysis, the Health and Medical Care Board has stated that the board has done

a needs and risk analysis, but only from the business perspective, not

from the integrity perspective. The Data Inspectorate therefore wants to emphasize that it

is not enough to do a needs analysis. As previously described,

appears from Article 32 of the Data Protection Ordinance and the National Board of Health and Welfare

regulations, it is required that the Health and Medical Care Board must also make one

risk analysis where the board considers various risks that may be associated with

one too at the availability of different types of personal data about patients for

to then weigh the needs of the business against the risks to the individual

integrity. In addition, the person responsible for personal data, according to i

the requirements of the Data Protection Regulation under Article 5, be able to

show that, among other things, appropriate organizational measures have been taken.

The Health and Medical Care Board has referred to the heads of operations

is responsible for a needs and risk analysis. The Data Inspectorate therefore wants

also emphasize that the board as the person responsible for personal data can not waive

take responsibility for the analysis and, on the basis of it, take appropriate technical and

organizational measures. This means that the board should have ensured

the implementation of a needs and risk analysis according to ch. § 2 HSLF-FS

2016: 40 and documented it.

A needs and risk analysis must be made at a strategic level

The Health and Medical Care Board has stated that the board after

The Data Inspectorate's previous injunction produced documents to provide

business managers tools for assigning permissions. The committee has

referred to the documents Guideline for information security - management and

operation and the template Template- Needs and risk analysis when allocating authorization

The Data Inspectorate states that the guidelines and the template are about

allocation of authorizations and that the documents are based on a need and

risk analysis must be done in connection with the actual allocation. (In the guidelines

states, for example, that a risk analysis must be performed to shed light on different types of risks

associated with too extensive availability and that documentation of

completed needs and risk analysis must be archived at the unit. In the template

referred to the Patient Data Act and that a decision on allocation must be preceded by a

needs and risk analysis). The Data Inspectorate therefore wants to emphasize that a

needs and risk analysis shall establish an overall competence structure

which in turn should form the basis for the allocation of qualifications to be made

for each individual executive. The strategic analysis to be taken is

thus further than the analysis made at the actual allocation of

the privileges. A properly conducted needs and risk analysis is one

prerequisite for the correct allocation of authorizations.

The Health and Medical Care Board has also referred to the documents

User profiles as examples of analyzes performed at actual

eligibility assignments. The Data Inspectorate also finds in this case that

it is not a question of any needs and risk analysis.

The Swedish Data Inspectorate's summary assessment

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

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

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

individual integrity that exists on both organizational and individual

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

provide a basis for an authorization structure that is adapted to the activities.

It should result in authorization assignments but it is not

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

In summary, the Data Inspectorate states that the Health and

the health care board has not submitted any documented needs and risk analysis. The committee has also stated that it has

not seen anyone

documented such. The Health and Medical Care Board has thus not been able to

show that the board has carried out a needs and risk analysis in the sense that

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

confidentiality or within the framework of coherent record keeping. This

means that the Health and Medical Care Board 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.

Authorization of access to personal data about patients

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

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

access to personal data about patients may be limited to

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

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

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

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

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

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

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

unauthorized dissemination of journal information within a business and should as

such is not accepted ”.

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

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

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

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

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

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

analyzes the risks to the individual's freedoms and rights

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

organizational measures needed to ensure no allocation

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

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

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

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

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

That the Health and Medical Care Board's allocation of qualifications does not have

preceded by a needs and risk analysis means that the board has not

analyzed users' needs for access to the data, the risks that

this access may entail and thus also not identified which

access that is justified to users based on such an analysis. The committee

has therefore not taken appropriate action in accordance with Article 32 of

the Data Protection Ordinance, to restrict users' access to

patients' personal data in the medical record system.

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

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

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

In the case, it has emerged that the number of registered patients in NCS Cross

within the internal secrecy is just over 650,000 and within the framework of

cohesive record keeping just over 665,000. The case has also emerged

that there are about 10,000 employees in the region and that just over 7,500

executives have been awarded Reading VLL in NCS Cross. This

authorization provides access (read access) to all devices

care documentation in the Västerbotten Region, except the one established on

protected devices. Of a total of 84 units, six are protected

devices. In summary, the Data Inspectorate states that this means

that the majority of employees have had actual access to

the care documentation on the majority of patients in NCS Cross.

Healthcare documentation means that it is a question of health information, so-called

sensitive personal data within the meaning of Article 9 (1) of the Data Protection Regulation. Through

that the personal data controller only restricted access to permissions

in NCS Cross to data available on protected devices it has thus

there has been a risk of unauthorized access and unauthorized distribution of

personal data partly within the framework of internal secrecy, partly within the framework

for the unified record keeping.

The Health and Medical Care Board has stated that an active choice for access is required

by the user when the patient has blocked their care documentation.

The Data Inspectorate wants to emphasize that an active choice is an enhancement of integrity

measure but does not constitute such an access restriction as referred to in ch. § 2

the Patient Data Act. This provision requires that the jurisdiction be limited

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

tasks in health care, ie. only those in need

the data must have access to them. Of the preparatory work for

Patient Data Act, prop. 2007/08: 126, p. 149, it appears that information in addition

need to be stored in different layers so that more sensitive data require active choices

or otherwise are not as easily accessible to staff as less sensitive

tasks.

Against this background, the Data Inspectorate can state that the Health and

the Health Care Board has processed personal data in violation of Article 5 (1) (f)

and Article 32 (1) and (2) of the Data Protection Regulation by the Board not

has restricted users' permissions to access the journal system

NCS Cross to what is only needed for the user to be able to fulfill

their duties in the health care system according to ch. § 2 and ch. 6 7

§ the Patient Data Act and ch. 4 2 § HSLF-FS 2016: 40. This means that the Health and Medical Care Board has not taken

measures to be able to ensure

and, in accordance with Article 5 (2) of the Data Protection Regulation, be able to display a

appropriate security for personal data.

Documentation of access (logs)

Based on the logs created as a result of the inspection

reviews together with the information provided by the board

the heading in the log extracts, the Data Inspectorate states that it off

the log extracts show the following:

- under the heading Activity, what measures have been taken with

information about a patient, for example to "read".

- under the headings Journal at which care unit or care process

measures have been taken

□

under the heading Time at which time the measures were taken

□

under the headings Patient and Personal the user's and the patient's

identity.

The Data Inspectorate finds that the documentation of the access (the logs)

in NCS Cross is in accordance with the requirements set out in ch. 9 § HSLF-

FS 2016: 40 and that the Health and Medical Care Board thus in this part has

have taken appropriate technical measures in accordance with Article 32 i

the Data Protection Regulation.

Choice of intervention

Legal regulation

If there has been a violation of the provisions of the Data Protection Regulation

the Data Inspectorate has a number of corrective powers available according to

Article 58 (2) (a) to (j) of the Data Protection Regulation. The supervisory authority may include

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

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

a specific period.

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

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

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

the circumstances of each individual case.

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

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

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

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

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

or 83.5 of the Data Protection Regulation.

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

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

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

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

duration. In the case of a minor infringement may

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

reprimand instead of imposing a penalty fee.

Order

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 health care, this means a great 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's inspection has shown that the Health and Medical Care Board has

failed to take appropriate security measures to provide protection to

personal data in the NCS Cross medical record system by not complying with the requirements

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

does not meet the requirements of Article 5 (1) (f) and Article 32 (1) and (2) (i)

the Data Protection Regulation. The omission includes both the inner

the secrecy according to ch. 4 the Patient Data Act as the cohesive one

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

The Data Inspectorate therefore submits, with the support of 58.2 d i

the Data Protection Ordinance, the Health and Medical Care Board to implement and

document the required needs and risk analysis for the NCS medical record system

Cross within the framework of both internal secrecy and within the framework of it

coherent record keeping. The Health and Medical Care Board shall further,

with the support of the needs and risk analysis, assign each user individually

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

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

Healthcare.

Penalty fee

The Data Inspectorate can state that the violations basically concern the Health and Medical Care Board's obligation to take

appropriate security measures for

to provide protection for personal data in accordance with the Data Protection Regulation.

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

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

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

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

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

notes that this is information that includes direct identification of

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

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

for example, family relationships, sexual life and lifestyle. The patient is addicted

of receiving care and is thus in a vulnerable situation. The nature of the data,

extent and the patients' position of dependence give caregivers a special

responsibility to ensure patients' right to adequate protection for their

personal data.

Additional aggravating circumstances are the treatment of

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

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

the possibility of access refers to a large proportion of the employees. In this case, stir

it is about 650,000 number of patients within the framework of the internal

confidentiality and about 665,000 patients under it

coherent record keeping. Of a total of 84 care units are available

restrictions on access to only six units, the so-called

protected devices.

The Data Inspectorate can also state that Health and

The Health Care Board did not follow the Data Inspectorate's decision of 27 March 2015.

The decision was presented to the then County Council Board in Västerbotten County

county council to carry out a documented needs and risk analysis accordingly

then requirement in ch. 2 § 6 second paragraph second sentence SOSFS 2008: 14,

which corresponds to the current provision in Chapter 4. 2 § HSLF-FS 2016: 40. This

is an aggravating circumstance, in accordance with Article 83 (2) (e) (i)

the Data Protection Regulation.

The shortcomings that have now been established have thus been known to Hälso- och

the health care board for several years, which means that the action has taken place

intentionally and thus is considered more serious. The Data Inspectorate

also notes that the Health and Medical Care Board's information that they

analyzes that have subsequently been made are solely based on the business perspective,

which is particularly serious.

In determining the seriousness of the infringements, it can also be stated that

the infringements also cover the basic principles set out in Article 5 (i)
the Data Protection Regulation, which is one of the more serious infringements that can
provide a higher penalty fee under Article 83 (5) of the Data Protection Regulation.
Taken together, these factors mean that are not to be judged as minor
infringements without infringements that should lead to an administrative
penalty fee.
The Data Inspectorate considers that these violations are closely related to
each other. That assessment is based on the need and risk analysis
form the basis for the allocation of the authorizations. The Data Inspectorate
therefore considers that these infringements are so closely linked
that they constitute interconnected data processing within the meaning of Article 83 (3) (i)
the Data Protection Regulation. The Data Inspectorate therefore decides on a joint
penalty fee for these infringements.
The administrative penalty fee shall be effective, proportionate and
deterrent. This means that the amount must be determined so that it
the administrative penalty fee leads to correction, that it provides a preventive
effect and that it is also proportional in relation to both current
violations as to the ability of the supervised entity to pay.
The maximum amount for the penalty fee in this case is SEK 10 million
according to ch. 6 Section 2 of the Act (2018: 218) with supplementary provisions to the EU
data protection regulation.
In view of the seriousness of the infringements and that the administrative
the penalty fee must be effective, proportionate and dissuasive
the Data Inspectorate determines the administrative sanction fee for
The Health and Medical Care Board to 2,500,000 (two million five hundred thousand)
kronor.

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

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

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

Katarina Tullstedt and Malin Blixt and the lawyer Caroline Cruz Julander

participated.

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

Appendix: How to pay a penalty fee

Copy for information to the Data Protection Officer

How to appeal

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

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

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

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

The Data Inspectorate forwards it to the Administrative Court in Stockholm

examination.

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

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

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