Decision

Diary no

2020-12-02

DI-2019-3841

The Health and Medical Services Board at

Region Västerbotten

Köksvägen 11

901 89 Umeå

Supervision according to the data protection regulation and

the patient data act — needs and risk analysis

and questions about access in medical records systems

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

The Swedish Data Protection Authority's decision

The Danish Data Protection Authority has during the review on 14 May 2019 and 12 December

In 2019, it was established that the Health Care Board at Region Västerbotten

processes personal data in violation of Article 5.1 f and 5.2 and Article 32.1

0ch 32.2 of the data protection regulation1 by

1.

The Health and Medical Services Board has not carried out needs and

risk analysis before assigning authorizations takes place in the records system

NCS Cross, in accordance with ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act

(2008:355) and ch. 4. § 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 healthcare. This means that Health and

the health care board has not taken appropriate organizational measures

in order to ensure and be able to demonstrate that the processing of

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

the risks.

2. The Norwegian Health and Welfare Board has not limited the users' rights

authorizations for access to the records system NCS Cross to what

only needed for the user to be able to fulfill their

duties within health care in accordance with

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

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

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

security of personal data.

Datainspektionen decides with the support of articles 58.2 and 83 i

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

supplementary regulations to the EU's data protection regulation that the Health and Medical Board, for the violations of article

5.1 f and 5.2 as well as

article 32.1 0ch 32.2 of the data protection regulation, must pay a

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

five hundred thousand) kroner.

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

Datainspektionen orders with the support of article 58.2 d i

the data protection regulation The Health and Medical Services Board to implement and

document the required needs and risk analysis for the records system NCS

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 duties

in healthcare, in accordance with Article 5.1 f and 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

have on site on 14 May 2019 and on 12 December 2019 reviewed whether the Health and Medical Services Board's decision

on the allocation of authorizations has been preceded

of a needs and risk analysis. The review has also covered how the Health and Medical Services Board assigned authorizations

for access to

the main records system NCS Cross, and what access capabilities they allocated

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

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

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

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

The Swedish Data Protection Authority has only reviewed the user's access options
the journal system, 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.).

Previous review of needs and risk analyses

The Swedish Data Protection Authority has previously carried out an inspection regarding the former
The County Council, Västerbotten County's County Council had carried out one
documented needs and risk analysis according to ch. 2 Section 6 second paragraph second
the meaning of the National Board of Health and Welfare's regulations (SOSFS 2008:14) re
information management and record keeping in healthcare. Of
The Data Inspectorate's decision with diary 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 according to the aforementioned regulations, and
was therefore recommended to implement one for the main journal system.

What emerged in the case

The Health and Medical Services Board has essentially stated the following.

Personal data controller

On 1 January 2019, a reorganization took place which meant that Region
Västerbotten was formed. There is no authority under Health and
the health care board. The Health and Medical Services Board conducts health and
healthcare within the region and is responsible for the processing of personal data

personal data that the business carries out in the main journal system NCS Cross.

Journal system

The main journal system used is called NCS Cross and stands for Nordic Clinical Suite. It is possible to access care documentation in NCS Cross from and including 1993 when the system was introduced. At that time was permission assignment more limited and users had access to fewer tasks than in today's system. The so-called Employee Assignments added in 2014–2015. The employee assignments regulate which organizational level access can occur in NCS Cross and is required to access the system.

NCS Cross is used within the framework of coherent record keeping along with seven other caregivers.

In connection with the data protection regulation starting to be applied did the supplier a general review of the system and informed that no functional adaptations had to be made.

There are 101 databases in NCS Cross based on the principle that every clinic has one own database. Within Region Västerbotten, 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 options different ways in terms of authorization control, including through the employee assignments and functions to block the journal.

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

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

for coherent record keeping is 665,564.

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

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

Cross. The number of active user accounts within 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 should be terminated. Access to NCS Cross

is still stopped because the users who do not have an employee assignment

unable to log into 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 confidentiality

Needs and risk analysis

From the Data Inspectorate's decision from 27 March 2015, it appears that

The County Council, Västerbotten County's county council, was instructed to produce one

documented needs and risk analysis for the main record system.

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

following.

The Health Care Board has followed the Data Inspectorate's previous decision

and produced the documents Guidelines for information security and

management and operation as well as Template – Needs and risk analysis at

authorization assignment. The guidance document and template have been established to provide

the operational managers tools in connection with the authorization assignment.

The User Profiles documents are examples that make it clear that permissions

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

carried out analyzes in the case of actual authority allocations within various

units.2 The needs and risk analysis is done based on the operational perspective and

not from the privacy perspective.

2

The documents have been received by the Swedish Data Protection Authority.

The board does not know to what extent the template Template – Needs and risk analysis

when assigning permissions is used out in the business, when you only see

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

the business managers carry out a needs and risk analysis before ordering

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

risk analysis neither for the internal secrecy nor for the cohesive one

record keeping.

The guidelines for information security state that authorization must be assigned

after an analysis of which information different personnel categories in different

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

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

a lot of access to various patient data. As the needs vary between different

types of operations, the operations manager is responsible for need- and

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

document the needs and risk analysis when assigning

employee assignment.

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

Authorization assignment regarding access to personal data about patients

The Health and Medical Services Board has essentially stated the following.

For an executive to be able to access personal data in NCS Cross several prerequisites need to be met. The executive must have one active user account in the region's domain (AD). This in turn presupposes that the executive is registered in the HR system. To be able to log in the domain requires executives to have a SITHS card with one or more valid ones certificate. In order to then be able to log in to NCS Cross, you need the executive partly has a valid so-called employee assignment, partly has become awarded a qualification in NCS Cross. The employee assignment regulates which organizational level access can take place in NCS Cross. It is the operational managers of the various units who decide on the allocation of employee assignment to their staff at the care unit.

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

The authority assigned to the staff is based on the needs analysis that is carried out prior to the assignment, i.e. 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 authorization to more devices. The same applies to emergency physicians who also have access to more units than the own emergency database.

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

Access possibilities (read permission) to care documentation in NCS Cross

Each employee has a reading authorization that is adapted based on the individual mission. If an employee is assigned reading authorization within the entire Region In Västerbotten, it only applies to care documentation. Protected devices are excluded.

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

Own authorization means that an executive is given access to them functions in the records system that are relevant to the executive tasks, for example prescribing medicines. Own authority also means that the executive is given read and write access to them parts of the records system (databases) that are connected to it or them care units where the executive is active.

Authorization according to Job role means that an executive is also given read access to other databases in the records system. The executive can then the service role Read permission VLL is given which means access possibility (read access) to all units' care documentation in the Region Västerbotten, except protected units. Executives can be assigned a

other reading permission than Reading permission VLL. Read permission to

personal data of protected entities is given only within the framework of assignment of

Own authority.

The module that manages the journal in NCS Cross is titled

Care documentation. The module contains all documentation available about

the patient in accordance with ch. 2 4 § 1 of the Patient Data Act. There are also others

modules, for example Care Administration which contain data in accordance

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

The doctors are almost always assigned Reading authorization VLL. Regarding

the nurses are often ordered Reading authorization VLL, which means that a

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

assigned write permission in the system means that the staff also have

read permission in it. The number of executives who have Reading authorization VLL i

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

124 are assistant nurses including children's nurses and 956 are paramedics.

The information applies to December 2019.

Restrictions on access to data in NCS Cross

There are no direct obstacles to introducing limiting functions

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

assigning permissions that give users different access possibilities.

It can be done on an individual level. You can also restrict access to some

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

access possibilities. The business managers can limit access and control permissions so that staff on a device only have access to data about care and treatment on the unit in question and not such information on others units.

Within NCS Cross 84 units are the following six protected units. 1) The device clinical genetics, 2) The unit child and youth rehabilitation 3) Section the child and youth habilitation within the child and youth clinic unit Västerbotten 4) Children's house section, within the children's unit youth psychiatry Västerbotten 5) Occupational health care 6) The LSS units within disability activities, Vision and hearing rehabilitation and Support and habilitation for adults and the exercise of authority section in the Support unit and habilitation for adults.

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

Coherent record keeping

The Health and Medical Services Board has essentially stated the following.

Needs and risk analysis

The template Template – Needs and risk analysis for authorization allocation also applies for the coherent record keeping. Needs analysis that is done before permission assignment also includes analysis for access within the context of coherent record keeping.

Authorization assignment regarding access to personal data about patients

If an employee has been assigned read permission in the internal confidentiality, it means

that he has also been assigned read permission for the coherent record keeping.

Access possibilities (read permission) to care documentation in NCS Cross

The read permission within the consolidated record keeping is the same as

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

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

coherent record keeping. As a basis for this lies

employee assignment.

Restrictions on access to data in NCS Cross

The employees must make active choices to access information in it

keep the records together, i.e. answer the question of whether the patient has given

their consent or alternatively state that there is an emergency in order to participate

of the data.

Documentation of the access (logs)

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

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

a patient can be registered on social security number or reserve number. According to

the guidelines, the system must select ten users out of one once a month

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

user opened for login during the checked log period as well

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

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

and date.

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

the measures have been taken, i.e. which care unit's employee assignment

the user used when logging in. Under the heading Journal it is stated

database from which the staff retrieved data, i.e. at which

care unit documentation the user reads.

The database called Medicincentrum contains care documentation from two

care units, partly Medical Centre, partly Heart Centre. If for example

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

the Medicincentrum unit, the log extract indicates Medicincentrum

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

however, working at Hjärtcentrum appears in the log extract under the heading

Client to be specified Hjärtcentrum.

The log entries generated relate to both the internal privacy and the

coherent record keeping.

The Health and Medical Services Board has submitted to the Data Inspectorate

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

reason for the inspection's review.

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 in 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 according to 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 when processing personal data.

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

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

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

supplementary rules, which must be applied when healthcare providers treat

personal data in healthcare.

National regulations that supplement the data protection regulation's requirements for

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

2016:40.

Requirements to carry out needs and risk analysis

The care provider must, according to ch. 4. § 2 HSLF-FS 2016:40 make a need-and

risk analysis, before assigning authorizations in the system takes place.

That an analysis of the needs as well as the risks is required is evident from the preparatory work

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

Authorization for the staff's electronic access to information about patients shall

is limited to what the executive needs to be able to carry out his duties

tasks within health care. It includes, among other things, that permissions should

are followed up and changed or reduced as changes in the individual

the executive's duties give reason for 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 more
information different personnel categories and different types of operations need. But
not only need analyzes are needed. Risk analyzes must also be done where you take
consideration of various types of risks that may be associated with an overly broad
availability regarding certain types of data. Protected personal data that is
classified as confidential, information about generally known people, information from some
receptions or medical specialties are examples of categories that can
require special risk assessments.

Generally speaking, it can be said that the more comprehensive an information system is, the
greater variety of different authorization levels there must be. Decisive for decisions about
authorization for e.g. different categories of healthcare professionals to
electronic access to data in patient records should be that the authorization must
limited to what the executive needs for the purpose of a good and safe
patient care. A more extensive or coarse-grained authorization assignment should –
although it would have points from an efficiency point of view - considered as one
unjustified dissemination of journal data within a business and should as such
not accepted.

Furthermore, data should be stored in different layers so that more sensitive data requires active
elections or otherwise are not as easily accessible to staff as less sensitive
tasks. In the case of personnel working with operational follow-up,
statistical production, central financial administration and similar activities
which is not individual-oriented, it should be enough for the majority of executives
access to data that can only be indirectly traced to individual patients.

directly pointing 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 take place, thus also apply 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 in 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 article 32 of the data protection regulation.

Article 32.1 states that the appropriate measures must be both technical and organizational and that 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 introduced, one has a lot

extensive digitization has taken place in healthcare. As well as the data collections
size as how many people share information with each other has increased
substantially. This increase means at the same time that the demands on it increase
personal data controller, because the assessment what is an appropriate
safety is affected by the extent of processing.

There is also the issue of sensitive personal data. The information concerns
people who are in a dependent situation when they are in need of care.
It is also often a question of a lot of personal data about each of these
people and the data may over time be processed by very
many people in healthcare. All in all, this places great demands on it
personal data controller.

The data that is processed must be protected against external actors as well
the business as against unauthorized access from within the business. It appears
of article 32.2 that the personal data controller, when assessing the appropriate
security level, in particular must take into account the risks of accidental or illegal
destruction, loss or for unauthorized disclosure or access. In order to
able to know what is an unauthorized access it must
personal data controller is clear about what constitutes an authorized access.

Needs and risk analysis

In ch. 4 § 2 The National Board of Health and Welfare's regulations (HSLF-FS 2016:40), which supplement
in the Patient Data Act, it is stated that the care provider must make a needs assessment
risk analysis before assigning authorizations in the system takes place. This means that
national law prescribes requirements for an appropriate organizational measure that shall
is taken before assigning authorizations to the record system takes place.

A needs and risk analysis must partly contain an analysis of the needs, partly a
analysis of the risks based on an integrity perspective that may be associated

with an excessively wide allocation of authorization for access to 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 integrity.

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

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

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

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

that it is a matter of protected personal data or general information

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

the preparatory work for the Patient Data Act shows that the more comprehensive one

information system is, the greater the variety of different authorization levels must be

there exist. (prop. 2007/08:126 p. 149).

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

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

updated.

In summary, the regulation requires that the risk analysis identifies

- different categories of data (for example, data about health),
- categories of data subjects (for example, vulnerable natural persons and

children), or

□

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

□

negative consequences for data subjects (e.g. damages,

significant social or economic disadvantage, deprivation of rights

and freedoms),

and how they affect the risk to the rights and freedoms of natural persons at

Processing of personal data. This also applies to internal confidentiality

as with coherent record keeping.

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

based on whether there are protected personal data that are

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

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

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

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

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

It is thus through the needs and risk analysis that it

data controller finds out who needs access, which

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

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

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

then lead to the technical and organizational measures needed to

ensure that no other access than that which is necessary and
the risk analysis shows is justified should be able to take place.
When a needs and risk analysis is missing prior to granting authorization i
system, there is no basis for the personal data controller on a legal basis
way must be able to assign their users a correct authorization. The
personal data controller is responsible for, and must have control over, it
personal data processing that takes place within the scope of the business. To
assign users a case of access to the record system, without this being established
on a performed needs and risk analysis, means that the personal data controller
does not have sufficient control over the personal data processing that takes place in
the record system and also cannot show that he has the control that
is required.
The Health and Medical Services Board's work with needs and risk analysis
When the Swedish Data Protection Authority has requested a documented need and
risk analysis, the Health and Medical Board has stated that the board has done
a needs and risk analysis, but only from the business perspective, not
based on the integrity perspective. The Swedish Data Protection Authority therefore wants to emphasize that it
it is not enough to carry out a needs analysis. As previously described,
appears from article 32 of the data protection regulation and the National Board of Health and Welfare
regulations, it is required that the Health and Medical Services Board must also make one
risk analysis where the board considers various risks that may be associated with
an excessively wide availability of different types of personal data about patients for
to then weigh the needs of the business against the risks for the individual
integrity. In addition, the personal data controller must, according to i
the data protection regulation's liability requirement according to Article 5, can
show that, among other things, appropriate organizational measures have been taken.

The Health and Medical Services Board has referred to the operational managers responsible for a needs and risk analysis being carried out. The Swedish Data Protection Authority therefore wants to also emphasize that the committee, as the person responsible for personal data, cannot waive itself the responsibility for the analysis and based on the appropriate technical and organizational measures. This means that the board should have ensured

the implementation of a needs and risk analysis according to ch. 4 § 2 HSLF-FS 2016:40 and documented it.

A need and risk analysis must be carried out at a strategic level

The Health and Medical Services Board has stated that the board after Datainspektionen's previous injunction produced documents to give the operational managers tools when assigning authorizations. The committee has referred to the documents Guideline for information security - management and operation and the template Template- Needs and risk analysis when assigning authorizations

The Swedish Data Protection Authority states that the guidelines and the template are about assignment 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 carried out to highlight different types of risks associated with for 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 decisions on allocation must be preceded by a needs and risk analysis). The Swedish Data Protection Authority therefore wants to underline that a needs and risk analysis must determine an overall authority structure

which in turn shall form the basis of the authorization assignment to be made

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

i.e. further than the analysis carried out during the actual allocation of

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

prerequisite for a correct assignment of authorizations.

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

User profiles as examples of completed analyzes in actual cases

authorization assignments. The Swedish Data Protection Authority also notes in this case that

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

The Swedish Data Protection Authority's summary assessment

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

the risks are assessed based on the information that needs to be processed in

the business, which processes it is a question of and which risks to it

individual integrity that exists both organizationally and individually

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

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

It should result in instructions on authorization assignment, but it doesn't

the instructions to the assigner of permissions which is the analysis.

In summary, the Data Inspectorate states that Health and

the medical board has not come in with any documented needs and risk analysis. The board has also stated that it has not

seen any

documented such. The Health and Medical Services 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, whether within the framework of the internal

confidentiality or within the framework of coherent record keeping. This

means that the Health and Medical Services Board 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.

Authorization assignment regarding access to personal data about patients

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

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

access possibilities to personal data about patients be limited to

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

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

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

2007/08:126 pp. 148-149, 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 extensive 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.

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

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

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

this access may entail and thus also not identified which

access that users are entitled to based on such analysis. The committee

has thus not used appropriate measures in accordance with Article 32 i

the data protection regulation, to limit users' access to

the patients' personal data in the record system.

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

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

confidentiality, partly within the framework of coherent record keeping.

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 scope of

consolidated record keeping of just over 665,000. In the case, it has also emerged
that there are around 10,000 employees within the region and that just over 7,500
executives have been assigned Reading authorization VLL in NCS Cross. This one
permission gives access (read permission) to all devices
care documentation in Region Västerbotten, except for the one drawn up on
protected devices. Out of a total of 84 units, six are protected
units. In summary, the Swedish Data Protection Authority states that it means
that the majority of employees have had actual access to
the care documentation for the majority of patients in NCS Cross.
Care documentation means that it is a matter of health data, so-called
sensitive personal data according to Article 9.1 of the data protection regulation. By
that the personal data controller only limited access to authorizations
in NCS Cross to data located on protected devices it has thus
there was a risk of unauthorized access and unauthorized dissemination of
personal data partly within the framework of internal confidentiality, partly within the framework
for the coherent record keeping.

The Health and Medical Services Board has stated that an active choice for access is required
by the user when the patient has blocked their care documentation.
The Data Inspection Authority wants to emphasize that an active choice is an increase in integrity
measure but does not constitute such an access restriction as referred to in ch. 4. Section 2
the patient data act. This provision requires the authorization to be limited
to what is needed for the individual to be able to fulfill their duties

tasks within health care, i.e. only those who need it

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

patient data act, prop. 2007/08:126, p. 149, it appears that data in addition

need to 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.

Against this background, the Data Inspectorate can state that Hälso- and

the health care board has processed personal data in violation of article 5.1 f

as well as article 32.1 0ch 32.2 of the data protection regulation in that the board does not

has restricted users' permissions to access the records system

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

their duties in health and medical care according to ch. 4. § 2 and ch. 6 7

§ the patient data act and ch. 4 Section 2 HSLF-FS 2016:40. This means that the Health 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 show a

appropriate security for the personal data.

Documentation of the access (logs)

Based on the logs that were created due to the inspection

reviews together with the information provided by the committee

the classification in the log extracts states that the

The log extracts show the following:

-

under the heading Activity, which measures have been taken with

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

-

under the headings Journal at which care unit or care process

the measures have been taken

- under the heading Time at which the measures were taken

- under the headings Patient and Personal the user's and the patient's identity.

The Swedish Data Protection Authority states that the documentation of the access (the logs) in NCS Cross is in accordance with the requirements set out in ch. 4. § 9 HSLF-

FS 2016:40 and that the Health and Medical Board therefore in this part has taken appropriate technical measures in accordance with Article 32 i data protection regulation.

Choice of intervention

Legal regulation

If there has been a violation of the provisions of the data protection regulation the Data Protection Authority has a number of corrective powers to access according to article 58.2 a - j of the data protection regulation. The supervisory authority can, among other things otherwise instruct the person in charge of personal data to ensure that the processing takes place 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.

For authorities, according to Article 83.7 of the Data Protection Regulation, national

rules state that authorities can impose administrative penalty fees.

According to ch. 6 § 2 of the Data Protection Act, penalty fees can be decided for

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

depending on whether the violation relates to articles covered by Article 83(4).

or 83.5 of the data protection regulation.

In Article 83.2 of the Data Protection Regulation, the factors to be taken into account are specified

to decide whether an administrative penalty fee should be imposed, but also

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

the assessment of the seriousness of the violation is its nature, severity and

duration. If it is a question of a minor violation may

the supervisory authority, according to recital 148 of the data protection regulation, issue a

reprimand instead of imposing a penalty fee.

Order

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.

Within health care, this means a great deal of 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 managers. 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

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

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's supervision has shown that the Health and Medical Services Board has

failed to take appropriate security measures to provide protection to

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

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

does not meet the requirements in Article 5.1 f and Article 32.1 and 32.2 i

data protection regulation. The omission includes the inner as well

confidentiality according to ch. 4 the Patient Data Act as the consolidated

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

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

the data protection regulation, the Health and Medical Board to implement and

document the required needs and risk analysis for the records system NCS

Cross within the framework of the inner secrecy as well as within the framework of it

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

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

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

which is needed for the individual to be able to fulfill his duties within

Healthcare.

Penalty fee

The Data Inspectorate can state that the violations basically relate to the Swedish Health and Medical Services Board's

obligation to take appropriate security measures for

to provide protection for personal data according to the data protection regulation.

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

personal data and extensive permissions. The caregiver needs to

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

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

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

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

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

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

for example, family relationships, sex 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' dependency status give care providers a special

responsibility to ensure patients' right to adequate protection for their

personal data.

Further aggravating circumstances are that the treatment of

personal data about patients in the main record system is at the core of a

care provider's activities, that the treatment includes many patients and

the possibility of access concerns a large percentage of the employees. In this case pipes

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

confidentiality and around 665,000 patients within its scope

coherent record keeping. Out of a total of 84 care units there are

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

protected the devices.

The Swedish Data Protection Authority can also state that Hälso- and

the health board did not follow the Data Inspection Authority's decision from 27 March 2015.

In the decision, the then County Council Board in Västerbotten County was presented

county council to carry out a documented needs and risk analysis according to it

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

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

is an aggravating circumstance, according to Article 83.2 e i

data protection regulation.

The deficiencies that have now been established have thus been known to Hälso- and

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

intentional and thus considered more serious. The Swedish Data Protection Authority

also states that the Health and Medical Services Board's statement that they

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

which is particularly serious.

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

the violations also include the fundamental principles of Article 5 i
the data protection regulation, which is among the more serious violations that can
give a higher penalty fee according to Article 83.5 of the Data Protection Regulation.
These factors together mean that is not to be judged as minor
violations without violations that shall lead to an administrative
penalty fee.
The Swedish Data Protection Authority believes that these violations are closely related to
each other. That assessment is based on the fact that the needs and risk analysis must
form the basis for the assignment of the authorizations. The Swedish Data Protection Authority
therefore considers that these violations are so closely related to each other
that they constitute connected data processing according to Article 83.3 i
data protection regulation. The Swedish Data Protection Authority therefore determines a joint
penalty fee for these violations.
The administrative penalty fee must be effective, proportionate and
deterrent. This means that the amount must be determined so that it
the administrative sanction fee leads to correction, that it provides a preventive measure
effect and that it is also proportionate in relation to current as well
violations as to the solvency of the subject of supervision.
The maximum amount for the sanction fee in this case is SEK 10 million
according to ch. 6 Section 2 of the law (2018:218) with supplementary provisions to the EU's
data protection regulation.
In light of the seriousness of the violations and that the administrative
the penalty fee must be effective, proportionate and dissuasive
the Data Inspectorate determines the administrative penalty fee for
The Health and Medical Board to 2,500,000 (two million five hundred thousand)
crowns.

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

presentation by IT security specialist Magnus Bergström. At the final

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

Katarina Tullstedt and Malin Blixt and the lawyer Caroline Cruz Julander

participated.

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

Appendix: How to pay 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 Swedish Data Protection Authority. Enter in

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

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

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

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

examination.

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

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

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