Decision

Diary no

2020-12-02

DI-2019-3843

Region Östergötland

To: The Regional Board

581 91 Linköping

Supervision according to the data protection regulation and

the patient data act – needs and risk analysis and

questions about access in records systems

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

Content

The Swedish Data Protection Authority's decision

The Swedish Data Protection Authority has, during its review on 10 April 2019, found that

The Regional Board, Region Östergötland (Regional Board) processes

personal data in violation of Article 5.1 f and 5.2, Article 24.1 and Article 32.1

0ch 32.2 of the data protection regulation1 by

1.

The Regional Board has not carried out a needs and risk analysis before

assignment of authorizations takes place in the journal system Cosmic, in accordance

with 4 ch. § 2 and ch. 6 Section 7 of the Patient Data Act (2008:355) and Chapter 4.

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

on record keeping and processing of personal data in health and

healthcare. This means that the Health and Medical Services Board does not have

taken appropriate organizational measures to be able to ensure

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

security that is appropriate in relation to the risks.

2. The Regional Board does not limit the user's authorizations for access

to the journal system Cosmic to what is only needed to

the user must be able to fulfill his tasks within health and

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

and ch. 4 Section 2 HSLF-FS 2016:40. This means that the Regional Board

have not taken measures to be able to ensure and be able to show one

appropriate security for the 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 provisions to the EU data protection regulation that

The Regional Board, for violation of article 5.1 f and 5.2 and article 32.1

and 32.2 of the data protection regulation, must pay an administrative

sanction fee of 2,500,000 (two million five hundred thousand) kroner.

The Swedish Data Protection Authority orders according to article 58.2 d of the data protection regulation

The Regional Board to implement and document the necessary needs and

risk analysis for the records system Cosmic 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

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).

fulfill their duties in health care, in accordance with

article 5.1 f and article 24.1 and article 32.1 and 32.2 of the data protection regulation,

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

Account of the supervisory matter

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

has on site on 10 April 2019 reviewed the Regional Board's decision on

allocation of authorizations, relating to the University Hospital in Linköping, has

preceded by a needs and risk analysis. The review has also covered how

The Regional Board assigned authorizations for access to the main records system

Cambio Cosmic (Cosmic), and what access possibilities they assigned

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

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

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

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

The Swedish Data Protection Authority has only reviewed users' access options
the journal system, i.e. which care documentation the user can actually take
part of and read. The review does not cover which functions are included in
the authorization, i.e. what the user can actually do in the records system
(e.g. signing, 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 County Council Board had carried out a documented needs and
risk analysis according to ch. 2 Section 6, second paragraph, second sentence of the National Board of Health and Welfare
regulations Information management and record keeping in health care
(SOSFS 2008:14). By the Data Inspectorate's decision with diary number 1600-2013,
announced on 27 March 2015, it appears that the County Council did not comply
the requirement to carry out a needs and risk analysis as mentioned
regulations. The County Council was therefore instructed to implement a
documented needs and risk analysis for the main record system.

What emerged in the case

The Regional Board has essentially stated the following.

Personal data controller

The Regional Board is a healthcare provider and responsible for personal data.

Journal system

Region Östergötland (the region) uses Cosmic as the main journal system
within the framework of the inner secrecy and participates in the Cosmic system of
coherent record keeping together with 20 private care providers. Cosmic

consists of a number of modules. The introduction of Cosmic began in February 2007 and was completed in December 2008, and the private care providers and coherent record keeping was added in 2009. Cambio is the supplier of this system.

The region is part of a customer group, "Kundgrupp Cosmic", which consists of eight regions and a private healthcare provider. These caregivers collaborate when it comes to development and requirements vis-à-vis the supplier Cambio, but each one of these care providers manage the operation of their own installation of the system.

The number of patients and employees

As of April 8, 2019, there were 838,093 unique patients registered in Cosmic. The figure is a total for all patients in Cosmic, i.e. the also includes the patients who are part of the system for cohesion record keeping.

In May 2019, there were 516,416 unique patients registered in Cosmic vid University Hospital in Linköping. As of September 7, 2019, the total had 7,014 executives at the University Hospital in Linköping access to Cosmic.

Internal confidentiality

Needs and risk analysis

The Regional Board has essentially stated the following.

There are three documents related to needs and risk analysis; Assessment of authorization allocation after a needs and risk analysis has been carried out (instructions and an overall guideline), Needs and risk analysis of permissions (the document refers to the assignment of permissions for employees within 12 centres) and Management of authorizations (guidelines for

assignment, change, removal and follow-up of authorizations i

the region's IT support).

From 2013 until 2015, discussions were held with the region regarding needs and risk analysis. A written needs and risk

analysis was available per centre

autumn 2015, which later resulted in the joint needs and

the risk analysis for all centers 2018. The document Assessment of

authorization assignment after a needs and risk analysis was determined by

decision of the Regional Board.

The purpose of the document Assessment of authorization assignment after execution

needs and risk analysis is to give clear instructions to those in charge

within each activity so that the assessments introduce

authority allocations take place uniformly within Region Östergötland. The

appears i.a. of the document that "the caregiver, i.e. The Regional Board,

responsible for each user being assigned an individual authorization for

access to patient data and that the allocation must be preceded by a needs and risk analysis. Each business manager or

equivalent must based on this

document and the guideline "Management of authorizations" carry out a needs and risk analysis for users within their own unit

and for those who

works on behalf of the operations manager. To the permissions in each

individual operations should neither be too broad nor too narrow

the operations manager has the opportunity to design the authorizations so that they

really correspond to the conditions of the individual business".

With regard to the risk analysis, the following appears. "The needs and risk analysis must

identify and list the mission of the business, the various occupational categories

that exist in the business as well as the tasks that the employee has in it

the business. Risks arising from the employee within the business

do not have access to relevant patient information must be identified and

listed in the needs and risk analysis and evaluated according to the current routine for

risk analysis. Furthermore, also risks related to too broad or generous access

to care information is identified and listed in the needs and risk analysis on

the same way as risks as above. The needs and risk analysis is used to

make sure that the authorization profiles that exist for each activity are

correct."

Furthermore, it is stated that "there are patient data and patient groups within

the region that is particularly worthy of protection, e.g. people with protected

personal data. It can be within the respective care unit or equivalent

there are additional patient data and patient groups that are special

worthy of protection e.g. based on care/diagnosis. The risks of accessing these

information needs to be highlighted in the needs and risk analysis".

The document Needs and risk analysis of authorizations is valid from now on

April 2019, and is version six of this document. The document contains, among other things,

information that all authorizations must be based on a need and

risk analysis where authorizations are limited to what is necessary to

employees must be able to perform their duties. This is to avoid a

improper dissemination of information but also for the employees to be right

conditions to be able to carry out their work. It also appears that a

a balancing of needs and risk must take place and that too wide an authorization may lead

to:

□

an unjustified dissemination of patient data/personal data

□

an economic risk

□

loss of accuracy in the form of incorrect deletion or alteration

information, as well as to

□

too narrow a permission may mean that the user cannot execute

their duties.

The following is specifically mentioned about Cosmic. “For permissions in Cosmic have

the need is grouped into user and professional roles. The risk of unauthorized

information dissemination has for each role been outweighed by the need for

information".

In the document Control of authorizations there are guidelines for control of

authorizations for the region's IT support.

During the inspection, the Regional Board stated that there was none

documented needs and risk analysis, but considered that the completed form

which concerns the ordering of authorizations is the result of a need-and

risk analysis. The Regional Board has subsequently come in with a point of view

this and stated that the document Assessment of authority allocation after

carried out needs and risk analysis constitutes a "basis for the risk analysis which is

completed. Completed form relating to ordering authorizations is based on

the assignment that the employee has and the authorization is given based on need and

risk".

Previous review of needs and risk analyses

To show how the Regional Board has acted according to the Data Inspectorate's past

decision against the County Board presented the document to the Regional Board

Assessment of authorization allocation after a needs and risk analysis has been carried out,

decided on 26 September 2016.

Authorization assignment for access to personal data

The Regional Board has essentially stated the following.

All permissions assigned to Cosmic are individual and there are none

group accounts.

Based on an executive's assignment and current care unit and

caregivers are made an order of authorization by the local administrator

on behalf of the operations manager. The operations manager's tasks in this

regard can be delegated to the head of the care unit, but the operations manager has

the ultimate responsibility for the order. This is given to those who work on

the support and is administered centrally.

There are different authorization profiles for different roles. An authorization profile

consists of a number of rights keys that are set per module in Cosmic. With

rights keys mean "keys in the system" that can be used to switch on

or of an authorization profile or to allocate a specific authorization profile.

The qualification profiles are in turn linked to different professional roles, which are based on

the executive's assignment.

A user's authorization profile determines which access possibilities and which

powers he has in the Cosmic. It is not possible to control if, for example, one

doctors can see a certain line in the Cosmic, this is done by the assignment of

rights keys. The rights keys mean that there is a technical

feature to fine-tune individual permissions, but that's general

seen so that different professional roles are assigned authorization profiles based on a matrix.

The matrix is advisory and provides suggestions for different authorization profiles in Cosmic

which may be suitable for different professional roles. From the matrix it appears that there is

22 authorization profiles based on user role and professional role. Two of these

authorization profiles are called "optional professional role". It is further clear from

the matrix that in practice all authorization profiles, apart from "Optional

professional role' in two respects, should be granted access to the Cosmic Modules

"Care documentation - Basic", "Drugs - Basic", "Referral - Basic" and

"Care administration - Basic".

Basic permission profiles in Cosmic

Care documentation – Basic: gives read and write rights to seven different

window, read permission in the Journal window, as well as permission "to read

Vital parameters in the patient overview".

Referral – Basic: gives read and write rights to five different windows, and

also includes read permission for medical information on referral.

The permission must be given to all users of the Referral module.

Medicines - Base: gives permission to open and read information in

the drug module and it also gives permission to open and read

information from "old" medicines; i.e. medication list,

enrollment decision, prescription list and prescription.

Assigned authorizations at the University Hospital in Linköping as of 7

September 2019

the Care documentation module: 6,221 users

the Medicines module: 6,102 users

the Referral module: 5,848 users

the Care Administration module: 5,956 users

During the inspection, it was stated that healthcare personnel - for example doctors,

nurses and assistant nurses, are assigned the authorization profile

"Care documentation - Basic", which means they can open medical records and

has read permission. It was also stated that no need and

risk analysis based on each authorization profile assignment. The Regional Board has

then came in with views on this and states the following.

"Care personnel can be assigned the authorization profile "Care documentation - Basic",

but it is not done automatically'. Furthermore, it is stated that "based on the guidelines

which are produced within Region Östergötland regarding

authorization control, etc. authorizations are assigned based on

needs and an underlying risk assessment."

Access to personal data about patients in Cosmic

The drug list in Cosmic is common. This means that everyone with

authorization has access to the drug list and to all the information available

where. However, it is possible to limit access to data i

the medication list.

Under the heading "All notes" in Cosmic are all journal entries

that has been written about the patient within the region. At the time of inspection

stated that the information under "All notes" is accessible to i

basically all nursing staff. The Regional Board has subsequently come in with one

point of view on this and states that access to "All Notes" requires

that the user has been assigned the "read journal entries" permission and that

an active selection is also required to bring up "All notes".

Restrictions on access to Cosmic regarding "All Notes" (Active

choice)

When it comes to selecting notes in Cosmic, it is done in the following way.

The Journal window opens and the user first ends up on “Unit's

notes”, which shows notes from the Medically Responsible Unit and

its subunits. Does the user want to read notes from other devices

within Region Östergötland or private healthcare providers who work on assignment

of the region an active choice is made, i.e. the user clicks on the heading “All

notes".

The following appears under “All notes”:

-

Caregiver's notes.

-

Some devices that are deemed to have extra sensitive information, i.e.

privacy around the device, displayed as Classified information.

Notes with extra sensitive information are displayed as

Classified information.

Other care provider is shown as Confidential information.

Private care provider is shown as Confidential information and

privacy is broken by the user clicking on the note and

answer Yes in the message box that appears. It is clear from the information

in the message box that the information is classified and to

gain access to the information, the confidentiality boundary needs to be broken. If

the information is written by another healthcare provider, consent is needed

from the patient unless it is an emergency. The user is then prompted

- Do you want to continue to access the information Yes/No/Cancel.

The rules regarding classified information govern how a note should be made

is presented and what action is required to access the information,

depending on which device wrote it and which device the user

who reads is logged in to. The user decides in the documentation

which secrecy class the note should belong to by choosing different

keyword templates. Particularly sensitive information has confidentiality class 4.1.

Privacy class on a template must be in parentheses after the template name, ex Curator (3)

and Curator (4.1). The rules regarding classified information are then specified

what action is required to break the confidentiality. In Region Östergötland

three levels are used:

No access with login

Create journal reference with logging

Warning with logging

The privacy class "No access with logging" means that
journal entries written on some devices cannot be read in Cosmic by it
own care provider (other than the specific unit to which it belongs) or by
other healthcare provider. To read notes from devices with this type of
classification, the user needs to receive business assignments for the unit,
which is decided by the operations manager. During the inspection it was stated that
there were three units within the University Hospital in Linköping that had this
confidentiality class: LSS Linköping, BUP Trauma units Linköping and Children
and the youth psychiatric clinic US. After the inspection, it has been received
supplementary information from the Regional Board where it appears that it
there has been a lowering of the secrecy class of the majority of the units within
BUP, but following a decision by the head of operations, it has been assessed that the trauma units must continue to have high
confidentiality without external access.
When there has been a declassification of a device that had No access
to get "normal" privacy (Warning with logging) the information becomes
readable. If it is a clinic within Region Östergötland that has lowered its
privacy, the user can read these notes via the All view
notes. For other caregivers, this means that the note is still

appears as classified information, but if they click on the note

then they get the information box "Show classified information", which

can be broken by clicking Yes after a consent is obtained.

The Create journal reference with logging privacy class means that if a

users from another business must read the note, they must

write a justification for why they are breaking confidentiality. This applies regardless of whether

the user works for the healthcare provider who drew up the journal entry or

with a healthcare provider who can see the note within its scope

coherent record keeping. If the note has been drawn up by a

another care provider's consent must also be obtained and documented beforehand

secrecy may be broken and the note may be read. However, it is not mandatory

but confidentiality can be broken even if this is not done.

After the inspection, the Swedish Data Protection Authority has received additional information

from the Regional Board concerning which units within the University Hospital i

Linköping which has the privacy class Create journal reference with logging, and

there are two care units: the Psychiatric Clinic in Linköping and

Psychiatry partners Children and Youth.

The privacy rule "Warning with logging" means that if a user on a

other business to read the note requires the user to click Yes i

a message box. This Yes means different things depending on whether

the note is written on a unit within the same healthcare provider (internal confidentiality)

or by another healthcare provider (joint record keeping).

Coherent record keeping

The Regional Board has essentially stated the following.

Needs and risk analysis

During the inspection, it was stated that there has not been a special needs assessment

risk analysis within the framework of the coherent record keeping.

The Regional Board considered that the needs and risk analysis carried out within the framework

for the inner secrecy also included the cohesive one

record keeping.

The Regional Board has subsequently come in with a point of view on this and

states that "the document Assessment of authority allocation after carried out

needs and risk analysis form a basis for the risk analysis that is

completed and also refers to coherent record keeping.

Authorization assignment

Happens in the same way as within the framework of internal secrecy.

Access to Cosmic

Within the framework of the coherent record keeping, the user must first

make an active choice before the user can share notes with others

healthcare providers. This means that a dialog box will appear where it says "show

classified data". If the user clicks in this box will

the notes to be displayed. The user must have consent from the patient

before that and that consent must, according to instructions, be documented by

the user in Cosmic.

Restrictions on access to Cosmic (Active Choices)

Some entities are excluded from coherent record keeping, either completely or

partly. It is not possible to break the privacy when the action "No access" has

been used.

Documentation of the access (logs)

The Regional Board has stated the following.

Documentation in the access logs from Cosmic:

-
-
-
-
-
-

information about the patient,

which user has opened the record (HSA ID and

user role),

what period of time someone was in the record,

time and date of last opening,

what measures have been taken,

from which care unit the user has been admitted.

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 source of law when processing personal data. This applies

also in health care.

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, implementing
appropriate technical and organizational measures to ensure and be able
show that the processing is carried out in accordance with the data protection regulation.
The measures must be implemented taking into account the nature of the treatment,
scope, context and purpose as well as the risks, of varying nature
degree of probability and seriousness, for the freedoms 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 for accidental or illegal destruction,
loss or alteration or to unauthorized disclosure of or unauthorized access to
the personal data transferred, stored or otherwise processed.
Recital 75 states that when assessing the risk of natural persons
rights and freedoms, different factors must be taken into account. Among other things are mentioned
personal data subject to confidentiality, information about health or
sexual life, if there is processing of personal data concerning vulnerable physical
persons, especially children, or if the treatment involves a large number
personal data and applies to a large number of registered users.
Furthermore, it follows from reason 76 that how probable and serious the risk for it
Data subjects' rights and freedoms should be determined based on the processing
nature, scope, context and purpose. The risk should be evaluated on
basis of an objective assessment, through which it is determined whether
the data processing involves a risk or a high risk.
Recitals 39 and 83 also contain writings that provide guidance on it
closer to the meaning of the data protection regulation's requirements for security at
Processing of personal data.
The Data Protection Regulation and the relationship with supplementary national
regulations
According to Article 5.1. a of the data protection regulation, the personal data must be processed
in a legal way. In order for the processing to be considered legal, legal is required
basis in that at least one of the conditions in Article 6.1 is met.
Provision of health care is one such task of generality
interest referred to in Article 6.1. e.
In healthcare, the legal bases can also be legal

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

updated.

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

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

6.2, retain or introduce more specific provisions to adapt

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

National law can further determine specific requirements for data processing

and other measures to ensure legal and fair treatment. But

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

duty; Article 6.3 states that the basis for the processing referred to in

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

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

special provision 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) as a general rule is prohibited.

Sensitive personal data includes information about health. In Article 9.2

the exceptions are specified when sensitive personal data may still be processed.

Article 9.2 h states that processing of sensitive personal data may take place if

the processing is necessary for reasons related to, among other things

provision of healthcare on the basis of Union law or

Member States' national law or according to agreements with professionals on

health area and provided that the conditions and safeguards which

referred to in point 3 are met. Article 9.3 requires regulated confidentiality.

This means that both the legal bases public interest,

exercise of authority and legal obligation such as treatment of sensitive

personal data with the support of the exception in Article 9.2. h needs

supplementary rules.

Supplementary national regulations

For Swedish purposes, both the basis for the treatment and the

the special conditions for processing personal data within health and

healthcare regulated in the Patient Data Act (2008:355), and

the patient data regulation (2008:360). In ch. 1 Section 4 of the Patient Data Act states that

the law supplements the data protection regulation.

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

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

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

personal data must be designed and otherwise processed so that patients' and

the privacy of other data subjects is respected. In addition, must be documented

personal data is handled and stored so that unauthorized persons do not gain access

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

The supplementary provisions in the Patient Data Act aim to

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

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

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

such as the right to personal integrity in the processing of personal data.

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

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

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

supplementary rules, which must be applied when healthcare providers treat

personal data in healthcare.

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

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

2016:40.

Requirements to carry out needs and risk analysis

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

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

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

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

Authorization for the staff's electronic access to information about patients must be limited to

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

healthcare. It includes, among other things, that authorizations must be followed up and changed or restricted accordingly

hand as changes in the individual executive's duties give rise to it.

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

inculcate the duty of the responsible health care provider to make active and individual

authorization assignments based on analyzes of which detailed information different

personnel categories and different types of operations need. But it is not only necessary

needs analyses. Risk analyzes must also be carried out where different types of risks are taken into account such as

may be associated with excessively wide availability regarding certain types of information.

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

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

may require special risk assessments.

Generally speaking, it can be said that the more extensive an information system is, the greater the quantity

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

categories of healthcare professionals to electronic access to records i

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

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

authorization assignment should - even if it would have points from an efficiency point of view - be considered as an unjustified

dissemination of medical records within an activity and as such should

not accepted.

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

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

applies to personnel who work with operational follow-up, statistical production, central

financial administration and similar activities that are not individual-oriented, probably

the majority of executives have access to information that can only be derived indirectly

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

information that directly points out individual patients should be able to be strong in this area

limited to single persons.

Internal confidentiality

The provisions in ch. 4 The Patient Data Act concerns internal confidentiality, i.e.

regulates how privacy protection must be handled within a healthcare provider's operations

and especially employees' opportunities to prepare access to

personal data that is electronically available in a healthcare provider's

organisation.

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

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

Coherent record keeping

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

Of ch. 6 Section 7 of the Patient Data Act follows that the regulations in ch. 4 § 2 also applies to assignment of authorization in case of joint record keeping. The requirement of that the care provider must carry out a needs and risk analysis before awarding authorizations in the system takes place, also applies in systems for cohesion record keeping.

Documentation of access (logs)

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

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

automatically documented and systematically checked.

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

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

actions taken with data about a patient;

2. the logs show which care unit or care process

the measures have been taken,

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

4. the identity of the user and the patient can be seen 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 they must ensure a level of security that is appropriate in

relation to the risks to the rights and freedoms of natural persons which

the treatment entails. It is therefore necessary to identify the possible ones

the risks to the rights and freedoms of the data subjects and assesses

the likelihood of the risks occurring and the severity if they occur.

What is appropriate varies not only in relation to the risks but also

based on the nature, scope, context and purpose of the treatment. It has

thus meaning what kind of personal data is processed, how many

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

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

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

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

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

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

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

personal data controller, because the assessment what is an appropriate

safety is affected by the extent of processing.

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

the patient data act states that the care provider must make a needs assessment

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

national law prescribes requirements for an appropriate organizational measure that shall

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

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

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

with an excessively wide allocation of authorization to access personal data

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

information that needs to be processed in the business, what processes it is

the question of whether and what risks exist for the individual's privacy.

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

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

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

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

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

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

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

comprehensive an information system is, the greater the variety

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

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

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

updated.

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.

Region Östergötland's process for needs and risk analysis

When the Swedish Data Protection Authority has requested a documented need and
risk analysis, the Regional Board has referred to three documents; Assessment of
authorization assignment after a needs and risk analysis has been carried out, Needs and
risk analysis of authorizations and Management of authorizations. The Swedish Data Protection Authority
can state that there are instructions and guidelines concerning the needs and risk analysis at the user level, which to some
extent tell how to proceed
prepare for the performance of a needs and risk analysis at the user level and
that a needs and risk analysis at user level must be done before allocation of
authorizations take place in the system. The Swedish Data Protection Authority can, however, further state
that the information in these documents is only presented at an overall level
for how to proceed before the execution of this analysis and that it
essential information is missing for a needs and risk analysis to be possible
performed in a correct manner. It is missing, e.g. an analysis of what need of
data different users have and an analysis of what risks are involved
access to, for example, certain categories of data or different types of
operations that contain sensitive data. Furthermore, the final one is missing

analysis that emerges when the need for data is weighted against the risk that
access to the data may entail. There is also a lack of analysis of
the business, the processes and an identified need for information from different
staff categories available at the Regional Board.
The Regional Board has had the opportunity to present a documented needs and risk analysis to the Data Inspectorate, but
has not been able to do this - either
itself within the framework of the internal secrecy or within the framework of it

coherent record keeping. The Regional Board believes that the document

Assessment of authority allocation after a needs and risk analysis has been carried out is one

needs and risk analysis and "constitutes a basis for the risk analysis which is

completed and completed form relating to ordering authorizations

is based on the assignment that the employee has and the authorization is given from the outside

need and risk, which also refers to coherent record keeping".

The Swedish Data Protection Authority can state that this document does not constitute an actual one

needs and risk analysis.

Authority allocation is in and of itself important organizational measures to

ensure proper access to personal data. A needs inventory constitutes

a stage in the work with a needs and risk analysis but it needs

supplemented by an assessment of the risks to patients' integrity and

thereby assessing and ensuring measures to manage the risks of unwarranted

spread.

Due to the above, the Swedish Data Protection Authority can state that

there is a lack of a documented needs and risk analysis that shows that

The Regional Board has carried out a needs and risk analysis in the sense that

referred to in ch. 4 § 2 HSLF-FS 2016:40, partly within the framework of internal confidentiality,

partly within the framework of the coherent record keeping according to 4 or 6 ch.

the patient data act. The documents that have been reported do not meet the requirements

which is based on a needs and risk analysis. As a result, the Regional Board does not have

nor able to demonstrate that assigned permissions are correct. This means a

considerable risk of unauthorized access to healthcare and patient data.

The personal data controller is responsible for following the basic

the principles of data minimization and appropriate security according to Article 5, 24

and 32 of the data protection regulation and has to show that the processing of

the personal data is processed in accordance with the data protection regulation.

The Regional Board, as the controller of personal data, has not complied

the liability according to Article 5.2 of the Data Protection Regulation by

be able to demonstrate that the regulations are complied with.

In light of the above, the Swedish Data Protection Authority can state that

The Regional Board at review on 10 April 2019 has processed

personal data in violation of Article 5.1 f and 5.2, Article 24.1 and Article 32.1

0ch 32.2 of the data protection regulation by not having fulfilled the requirement to

carry out a needs and risk analysis before assigning authorizations i

the journal system Cosmic in accordance with ch. 4 § 2 and ch. 6 Section 7

the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40. This means that

The Regional Board has not taken appropriate organizational measures to

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

a security that is suitable in relation to the risks.

Authorization assignment regarding access to personal data about patients

As has been reported, a caregiver may have a legitimate interest in having one

extensive processing of information about individuals' health. Regardless of this shall

access possibilities to personal data about patients be limited to

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

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

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

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

the journal system and that the authorizations must be limited to what the user

need to provide the patient with good and safe care. It also appears that "one

more expansive or coarse-grained authority assignment should be considered a

unjustified dissemination of medical records within a business and should as

such is not accepted."

In healthcare, it is the person who needs the data in their work

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

caregivers as between caregivers. It is, as previously mentioned, through the needs and risk analysis that the personal data

controller finds out who

need access, what data the access should cover, at what times

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

risks to the individual's freedoms and rights that the processing may lead to.

The result must then lead to the technical and organizational measures that

needed to ensure that the assignment does not provide further access opportunities

than the need and risk analysis shows is justified. An important

organizational action is to give direction to those who have the authority to

assign permissions on how this should be done and what should be taken into account so that

that, with the needs and risk analysis as a basis, becomes a correct one

authorization assignment in each individual case.

It appears that in Cosmic there are four modules that contain

personal data: "Care documentation - Basic", "Drugs - Basic",

"Care administration - Basic" and "Referral - Basic". The Regional Board has stated

that of 7,014 users at the University Hospital in Linköping, 6,221 have

user assigned basic access to the Care documentation module, 6 102

user has been assigned basic access to the Medicines module, 5,956

users have been assigned basic access to the Care Administration module and 5

848 users have been granted basic access to the Referral module. This means

that a majority of users have been granted access to the four

the modules of Cosmic.

As far as limitations in Cosmic are concerned, the Regional Board has exclusive rights

explained the personal data found under "All notes" i

the "Care documentation" module. The Regional Board has stated that there are three

types of classified information and that users have the opportunity to

classification information regarding two of these three classification classes.

Regarding the privacy class "No access with logging", this takes place

classification of the caregiver. There are two units at the University Hospital i

Linköping whose information has received this confidentiality class. The Swedish Data Protection Authority

notes that a real limitation of user access has taken place in these

case.

As for the other two privacy classes, “Create journal reference with

logging" and "Warning with logging", are the personal data that have been requested

with this "privacy" still electronically accessible through active selection.

By clicking the consent or emergency access box, the user can

this still access all personal data, which means that everyone

users who make these active choices can access patients' data and

not only the users who have a need.

Of the preparatory work for the Patient Data Act, prop. 2007/08:126, p. 149, it appears that

the purpose of the provision on access restriction in ch. 4. Section 2

the patient data act is to inculcate the obligation of the responsible healthcare provider

to make active and individual authorization assignments based on analyzes of

which detailed information different staff categories and different types

businesses need. It appears from the preparatory work that data should also

stored in different layers so that more sensitive data requires active choices or else

are not as easily accessible to staff as less sensitive data.

That the Regional Board uses the above active elections is one

privacy-enhancing measure, but does not mean that these active choices constitute one

such access restriction as referred to in ch. 4 Section 2 of the Patient Data Act. This one

provision requires that the authorization be limited to what is needed for

that the individual must be able to fulfill his duties within health and

healthcare, i.e. only those who need the data should have access, and

no such limitation has occurred. The Swedish Data Protection Authority also questions

The Regional Board's approach when it comes to the users themselves

classified information, and not the Regional Board itself.

The Regional Board has exclusively given an account of the personal data that exists

under "All notes" in the module "Care documentation" where applicable

the possibility for the user to classify information as confidential. Otherwise have

The Regional Board did not state that there are any limitations or

confidentiality classes regarding other personal data or in other modules.

On the contrary, the Regional Board has e.g. stated that anyone who has access to

Cosmic has access to the “Medicine – Base” module, even if it exists

possibility to restrict access to the data in this module.

Because different users have different tasks within different

work areas, need user access to the data in Cosmic

be limited to reflect this. The Regional Board has, apart from them
information that has been given the privacy class "No access with logging", not
limited user permissions for access to patients
personal data in the record system, whether within the framework of the internal
the confidentiality or within the framework of the coherent record keeping i
the Cosmic system. This means that a majority of users at
The University Hospital in Linköping, which has access to Cosmic, also has
access to a majority of the personal data contained in the four modules.
The users' authorizations have thus not been restricted in such a way as
the provisions of the Patient Data Act require and the Regional Board has not, i
in accordance with Article 32, used sufficient technical measures to
restrict users' access to personal data i
the journal systems to only what is needed for the user to be able to
fulfill their duties. This means that the assignment of permissions
has been too extensive, general and carried out for one for the personal
the integrity of intervening ways and thereby been disproportionate i
relation to the purpose.

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
the confidentiality, which includes 516,416 patients, partly within the framework of it
coherent record keeping, which includes 838,093 patients. The number
users are 7,014 and the number of users who have been granted access to
the data in the various modules is between 5,848 – 6,221.

It appears that the Regional Board has not limited health and

access possibilities of healthcare professionals and medical secretaries to

information about patients either within the framework of internal confidentiality or

within the framework of coherent record keeping in the Cosmic record system.

Against the background of the above, the Swedish Data Protection Authority can state that

The Regional Board at review on 10 April 2019 has processed

personal data in violation of Article 5.1 f and 5.2, Article 24.1 and Article 32.1

0ch 32.2 of the data protection regulation in that the Regional Board has not

restricted users' permissions for access to the Cosmic journal system

to only what is needed for the user to be able to fulfill their

duties within health and medical care according to ch. 4 § 2 and ch. 6 Section 7

the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40. This means that

The Regional Board has not taken measures to be able to ensure and

be able to demonstrate appropriate security for the personal data.

Documentation of the access (logs)

The Swedish Data Protection Authority can state that it appears from the logs in Cosmic

information about the specific patient, which user has opened

the journal, actions taken, which journal entry has

opened, what time period the user has been in, all openings of

the record made on that patient during the selected time period and

time and date of last opening.

Datainspektionen has nothing to recall in this part, because

The Regional Board meets the requirements for the content of documentation in the logs

which appears from ch. 4. § 9 HSLF-FS 2016:40 and has thus taken

appropriate technical measures according to Article 32 of the Data Protection Regulation,

Choice of intervention

Legal regulation

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

Datainspektionen a number of corrective powers to be available according to article

58.2 a - j of the data protection regulation. The supervisory authority can, among other things

order the personal data controller to ensure that the processing takes place in

in accordance with the regulation and if required in a specific manner and within a

specific period.

From article 58.2.i and article 83.2 of the data protection protection regulation it appears that

The Swedish Data Protection Authority has the authority to impose administrative penalty fees

in accordance with Article 83. Furthermore, it appears that depending on the circumstances i

the individual case, administrative penalty fees shall be imposed in addition to or in

instead of the other measures in Article 58.2.

For authorities, according to Article 83.7 of the data protection regulation, national

rules state that authorities can impose administrative penalty fees.

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

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

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

or 83.5 of the data protection regulation.

Article 83(2) sets out the factors to be taken into account in deciding whether a

administrative penalty fee shall be imposed, but also what shall affect

the amount of the penalty fee. Of central importance for the assessment of

the seriousness of the breach is its nature, severity and duration. If

it is a question of whether a minor violation gets the supervisory authority, according to reason

148 of the Data Protection Regulation, issue a reprimand instead of imposing one
penalty fee.

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 executives. Equally important is that

there is an actual analysis of the risks based on an integrity perspective
can occur in the event of an excessive assignment of authorization to access. From
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.

In this case, the Regional Board has failed to carry out a needs and

risk analysis, something that is directly prescribed in ch. 4. Section 2 HLSF-FS 2016:40. The
means that the Regional Board has had no basis for assessing which
itself the need or the risk when authorization is granted. It has also led to
access for employees has not been limited to what is needed to
the individual must be able to fulfill his duties within health and
healthcare. This also applies to access within the internal confidentiality according to ch. 4.
the patient data act as the coherent record keeping according to ch. 6
the patient data act.

The Swedish Data Protection Authority therefore orders according to Article 58.2 d i
the data protection regulation The Regional Board to implement and document
required needs and risk analysis for the records system Cosmic and that
then, based on 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 within
health care, in accordance with article 5.1 f and article 24.1 and article
32.1 and 32.2 of the data protection regulation, ch. 4 § 2 and ch. 6 Section 7
the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40.

Penalty fee

The Data Protection Authority can state that the violations relate to the Regional Board's
obligation to protect personal data with appropriate security measures
according to article 32 of 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
patient data in the master record system is at the core of a healthcare provider's
operations and treatment include many patients and the possibility of
access refers to a large percentage of employees. In this case, it is 516,416
unique patients within the framework of internal confidentiality, and 794,626 unique
patients within the framework of the integrated record keeping. There is
only two devices where the data is not accessible to the users outside
these units.
It has also emerged that the Regional Board has not remedied it before
the order from the Data Inspectorate, dated 27 March 2015, there
The Regional Board was instructed to produce a documented needs and
risk analysis that fulfilled the then requirement ch. 2 Section 6, second paragraph
second sentence SOSFS 2008:14, which corresponds to the current provision in 4
Cape. Section 2 HSLF-FS 2016:40. This is, according to article 83.2 e
the data protection regulation, to be considered as an additional aggravating factor

circumstance.

The Swedish Data Protection Authority notes that the deficiencies that have now been identified have been known to the Regional Board for several years, which means that the action was done intentionally and is therefore considered more serious.

When determining the seriousness of the violations, it can also be established that the violations also refer to article 5, which is stated to be among the more serious the violations that may result in a higher penalty fee according to Article 83.5.

Taken together, these factors mean that the violations in question are not to judge as minor violations without the violations shall lead to a 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.

Based on the seriousness of the violations and that the administrative penalty fee

must be effective, proportionate and dissuasive determines

The Data Inspectorate the administrative sanction fee for the Regional Board

to 2,500,000 (two million five hundred thousand) kroner.

_____

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

presentation by IT security specialist Magnus Bergström. At the final

the handling is handled by chief legal officer Hans-Olof Lindblom, the unit managers

Katarina Tullstedt and Malin Blixt and the lawyer Maja Savic participated.

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

Appendix 1 – How to pay penalty fee

Copy for the attention of:

Data Protection Officer

3 0 (31)

The Swedish Data Protection Authority

DI-2019-3843

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.