Decision

Diarienr

2020-12-02

DI-2019-3843

Östergötland Region

Att: Regional Board

581 91 Linköping

Supervision in accordance with the Data Protection Regulation and

Patient Data Act - needs and risk analysis and

questions about access in journal systems

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00



Content

The Data Inspectorate's decision

During an inspection on 10 April 2019, the Data Inspectorate has established that

The Regional Board, Östergötland Region (Regional Board) deals with

personal data in breach of Article 5 (1) (f) and (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

allocation of permissions takes place in the journal system Cosmic, in accordance

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

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

on record keeping and processing of personal data in health and

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

have taken appropriate organizational measures to ensure

and be able to show that the processing of personal data has one

security appropriate to the risks.

2. The Regional Board does not limit users' permissions for access

to the journal system Cosmic to what is only needed to

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

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

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

have not taken steps to be able to secure and be able to show one

appropriate security for personal data.

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

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

additional provisions to the EU Data Protection Regulation that

The Regional Board, for violation of Article 5 (1) (f) and (2) and Article 32 (1)

and 32.2 of the Data Protection Regulation, shall pay an administrative

penalty fee of 2,500,000 (two million five hundred thousand) kronor.

The Data Inspectorate submits in accordance with Article 58 (2) (d) of the Data Protection Regulation

The Regional Board to implement and document the necessary needs and

risk analysis for the Cosmic record system and to subsequently, with the support of the needs and risk analysis, assign each

user individual access rights

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 protection

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

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

Data Protection Regulation).

1



perform their duties in health care, in accordance with

Article 5 (1) (f) and Article 24 (1) and Article 32 (1) and (2) of the Data Protection Regulation;

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

Report on the supervisory matter

The Data Inspectorate initiated the inspection by letter dated 22 March 2019 and

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

allocation of qualifications, which concerns the University Hospital in Linköping, has

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

The Regional Board has granted authorizations for access to the main record system

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

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

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

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

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

The Data Inspectorate has only examined users' access possibilities to

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

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

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

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

Previous review of needs and risk analyzes

The Data Inspectorate has previously carried out an inspection regarding

The County Council Board had carried out a documented needs and

risk analysis according to ch. 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). Of the Data Inspectorate's decision with record number 1600-2013,

announced on March 27, 2015, it appears that the County Council Board did not comply

the requirement to carry out a needs and risk analysis according to the said

regulations. The County Council Board was therefore instructed to implement one

documented needs and risk analysis for the main record system.



What has emerged in the case

The Regional Board has mainly stated the following.

Personal data manager

The Regional Board is the care provider and person responsible for personal data.

Journal system

Region Östergötland (the region) uses Cosmic as the main journal system

within the framework of internal confidentiality and participates in Cosmic's system for

cohesive record keeping together with 20 private care providers. Cosmic

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

The region is part of a customer group, "Customer group Cosmic", which consists of eight regions and a private care provider. These caregivers cooperate when it comes to development and requirements towards the supplier Cambio, but each of these care providers take care of the operation of their own installation of the system.

The number of patients and employees

On April 8, 2019, there were 838,093 unique patients registered in Cosmic. The figure is a total for all patients in Cosmic, ie. the also includes the patients included in the cohesion system record keeping.

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

Internal secrecy

Needs and risk analysis

The Regional Board has mainly stated the following.

There are three documents that are attributable to needs and risk analysis; Assessment of eligibility allocation after performing needs and risk analysis (instructions and an overall guideline), Needs and risk analysis of authorizations (the document refers to the allocation of authorizations for employees within 12 centers) and Management of authorizations (guidelines for

allocation, change, removal and follow-up of authorizations in

the region's IT support).

From 2013 to 2015, discussions were held in the region regarding needs and risk analysis. A written needs and risk analysis was available per center from

in the autumn of 2015, which later resulted in the joint needs and

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

eligibility allocation after performing needs and risk analysis was determined by

decision of the Regional Board.

Purpose of the document Assessment of authorization allocation after completed

needs and risk analysis is to give clear instructions to those responsible

within each activity so that the assessments introduce

Eligibility allocations are made uniformly within the Östergötland Region. The

emerges i.a. of the document that “the caregiver, ie. The Regional Agency,

is responsible for assigning each user an individual authorization for

access to patient data and that the allocation must be preceded by a needs and risk analysis. Each operations manager or equivalent must be based on this

documents and the guideline "Management of permissions" carry out a needs and risk analysis for the users within their own unit and for those who

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

individual business should not be too wide or too narrow needs

the business manager have the opportunity to design the permissions so that they

really corresponds to the conditions of the individual business ”.

With regard to the risk analysis, the following is clear. “The needs and risk analysis shall

identify and list the business's assignments, the different occupational categories

that are in the business and the assignments that the employee has in

the business. Risks that arise about 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 valued according to the current routine for

risk analysis. Furthermore, there must also be 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

ensure that the eligibility profiles available for each activity are

correct. ”

It is further stated that “there are patient data and patient groups within

the region that are particularly worthy of protection e.g. persons with protected

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

there are additional patient data and patient groups that are specific



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

April 2019, and is version six of this document. The document contains i.a.

information that all competencies should be based on a needs and

risk analysis where the privileges are limited to what is necessary to

employees must be able to perform their tasks. This is to avoid one

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

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

balancing of needs and risks must take place and that one can lead to eligibility

to:

□

an unjustified dissemination of patient data / personal data

□

a financial risk

□

lost accuracy in the form of incorrect erasure or altered

information, and that

□

a too narrow jurisdiction may mean that the user can not perform

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 use dissemination of information has for each role been offset by the need for information".

The document Management of permissions contains guidelines for control of qualifications for the region's IT support.

During the inspection, the Regional Board stated that there was none documented needs and risk analysis, but considered the completed form relating to the ordering of authorizations is the result of a need and risk analysis. The Regional Board has since submitted a comment on this and stated that the document Assessment of eligibility allocation after performed needs and risk analysis constitutes a “basis for the risk analysis that is implemented. Completed form relating to ordering permissions is based on the assignment that the employee has and the authority is given based on needs and risk".

Previous review of needs and risk analyzes

To show how the Regional Board has acted after the Data Inspectorate's earlier

decision against the County Council Board, the Regional Board presented the document



Assessment of eligibility allocation after performing needs and risk analysis,

decided on 26 September 2016.

Authorization assignment for access to personal data

The Regional Board has mainly stated the following.

All privileges assigned to Cosmic are individual and there are none

group accounts.

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

caregivers, an order for authorization is made by the local administrator

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

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

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

support and administered centrally.

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

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

rights keys are "keys in the system" that can be used to turn on

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

The eligibility 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 options and which

powers this has in Cosmic. It is not possible to redirect, for example, one

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

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

function to control individual privileges in detail, but it is general

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

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

which may be suitable for different professional roles. The matrix shows that it exists

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

eligibility profiles are called "optional professional role". It is further stated by

the matrix that in practice all eligibility profiles, except “Optional

professional role ”in two respects, should be granted access to the Cosmic modules

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

"Care administration - Basic".

Basic eligibility profiles in Cosmic



Care documentation - Basic: provides reading and writing rights to seven different ones

window, reading right in the Journal window, and permission to read

Vital parameters in the Patient Overview ”.

Referral - Basic: provides read and write permissions to five different windows, and

also includes read access for medical information on referral.

The authorization must be given to all users of the Referral Module.

Medicines - Basic: 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. the drug list,

enrollment decision, prescription list and prescription.

Awarded eligibility at the University Hospital in Linköping as of the 7th

September 2019

module Care documentation: 6 221 users

module Pharmaceuticals: 6,102 users

module Referral: 5,848 users

module Care Administration: 5,956 users

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

nurses and assistant nurses, are assigned the eligibility profile

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

has reading permission. It was also stated that no needs and no

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

then submitted comments on this and states the following.

"Care staff can be assigned the eligibility profile" Care documentation - Basic ",

but it is not done automatically ". It is further stated that "based on the guidelines

which are produced within Region Östergötland regarding

authorization control etc. an allocation of permissions is made based on

needs and an underlying risk assessment. "

Access to personal data about patients in Cosmic

The list of medicines in Cosmic is common. That means everyone with

authority has access to the list of medicines and to all available information

where. However, it is possible to restrict access to data in

the drug list.

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

which 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 healthcare staff. The Regional Board has since come in with one

comment on this and states that access to "All Notes" requires



that the user has been granted permission to "read journal entries" and that

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

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

choice)

When it comes to choosing notes in Cosmic, the procedure is as follows.

The Journal window opens and the user first enters the “Device's

notes ”, which shows notes from the Medical Unit and

its subunits. The user wants to read notes from other devices

within Region Östergötland or private care providers who work on assignment

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

notes".

The following is displayed under "All notes":

- 

The caregiver's notes.

- 

Some devices that are judged to have extra sensitive information, ie.

privacy around the device, is displayed as Privacy-rated information.

Notes with extra sensitive information are displayed as

Classified information.

Other care providers are displayed as classified information.

Private care providers are displayed as classified information and

the privacy is broken by the user clicking on the note and

answers Yes in the message box that appears. It appears from the information

in the message box that the information is classified and to

access to the information, the confidentiality limit needs to be broken. If

the information is written by another caregiver needs consent

from the patient unless there is an emergency. The user is then asked the question

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

The rules regarding classified information govern how a note should be

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 on the documentation

which privacy class the note should belong to by choosing different

keyword templates. Particularly sensitive information is classified 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 then state

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

three levels are used:

No access with logging

Create journal reference with logging

1 0 (31)

The Data Inspectorate

DI-2019-3843

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 (in addition to the specific unit to which it belongs) or by

another care provider. To read notes from devices with this type of

confidentiality classification, the user needs to be given business assignments to 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 U.S. Department of Adolescent Psychiatry. After the inspection, it has arrived

supplementary information from the Regional Board where it appears that it

there has been a reduction in the secrecy class of most of the units within

BUP, but following a decision from the head of operations, it has been judged that the Trauma Units will continue to have high

confidentiality without external access.

When there has been a privacy snag on a device that has had No access

to get "normal" confidentiality (Warning with logging) becomes the information

readable. If it is a clinic within the Östergötland Region 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 there

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 has been obtained.

Privacy class Creating journal reference with logging means that if one

users from another business should read the note so he must

write a motivation for why they are violating confidentiality. This applies regardless of

the user works for the care provider who drew up the medical record or

at a care provider who can take note of the note within the framework of it

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

other care providers must also obtain consent and document it beforehand

confidentiality may be breached and the note may be read. However, it is not mandatory

without secrecy can be broken even if this is not done.

After the inspection, the Data Inspectorate has received supplementary information

from the Regional Board regarding which units within the University Hospital in

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

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

Psychiatric partners Children and Adolescents.



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

other business should read the note requires the user to click Yes in

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

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

or by another care provider (coherent record keeping).

Coherent record keeping

The Regional Board has mainly stated the following.

Needs and risk analysis

During the inspection it was stated that no special needs and

risk analysis within the framework of the coherent record keeping.

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

for the internal secrecy also included the cohesive

record keeping.

The Regional Board has since submitted a comment on this and

states that “the document Assessment of eligibility assignment after completed

needs and risk analysis forms the basis for the risk analysis that is

implemented and also refers to coherent record keeping.

Eligibility

Takes place in the same way as within the framework of internal secrecy.

Access to Cosmic

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

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

healthcare providers. This means that a dialog box appears where it says “show

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

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

before that and that consent must be documented by instructions

the user in Cosmic.

Restrictions on access to Cosmic (Active Choices)

Some units are outside the coherent record keeping, either completely or completely

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

used.

Documentation of access (logs)

The Regional Board has stated the following.



Documentation in the access logs from Cosmic:

- 
- 
- 
- 
- 
- 

patient information,

which user has opened the journal (HSA ID and

user role),

what period of time someone has been in the journal,

time and date of last opening,

what measures have been taken,

from which care unit the user has been inside.

Justification of the decision

Applicable rules

The Data Protection Regulation is the primary source of law

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

is the primary source of law in the processing of personal data. This applies

also in health care.

The basic principles for processing personal data are set out in

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

security pursuant to Article 5 (1) (f), which states that personal data shall be processed
in a way that ensures appropriate security for personal data,
including protection against unauthorized or unauthorized treatment and against loss;
destruction or damage by accident, using appropriate
technical or organizational measures.
Article 5 (2) states the so-called liability, ie. that it
personal data controllers must be responsible for and be able to show that the basics
the principles set out in paragraph 1 are complied with.
Article 24 deals with the responsibility of the controller. Of Article 24 (1)
it appears that the person responsible for personal data is responsible for implementing
appropriate technical and organizational measures to ensure and be able to
demonstrate that the processing is performed in accordance with the Data Protection Regulation.
The measures shall be implemented taking into account the nature of the treatment,
scope, context and purpose as well as the risks, of varying
probability and seriousness, for the freedoms and rights of natural persons,
The measures must be reviewed and updated as necessary.

Article 32 regulates the security of the processing. According to paragraph 1
the personal data controller and the personal data assistant shall take into account
of the latest developments, implementation costs and treatment
nature, scope, context and purpose as well as the risks, of varying
probability and seriousness, for the rights and freedoms of natural persons
take appropriate technical and organizational measures to ensure a
level of safety appropriate to the risk (…). According to paragraph 2,

when assessing the appropriate level of safety, special consideration is given to the risks
which the treatment entails, in particular for accidental or unlawful destruction,
loss or alteration or to unauthorized disclosure of or unauthorized access to
the personal data transferred, stored or otherwise processed.
Recital 75 states that in assessing the risk to natural persons
rights and freedoms, various factors must be taken into account. Among other things mentioned
personal data covered by professional secrecy, health data or
sexual life, if the processing of personal data concerning vulnerable physical persons takes place
persons, especially children, or if the treatment involves a large number
personal data and applies to a large number of registered persons.
Furthermore, it follows from recital 76 that the likelihood and seriousness of the risk for it
data subjects' rights and freedoms should be determined on the basis of processing
nature, scope, context and purpose. The risk should be evaluated on
on the basis of an objective assessment, which determines whether
the data processing involves a risk or a high risk.
Recitals 39 and 83 also contain writings that provide guidance on it
the meaning of the Data Protection Regulation's requirements for security in
Processing of personal data.
The Data Protection Regulation and the relationship with complementary national
provisions
According to Article 5 (1). In the Data Protection Ordinance, personal data must be processed
in a legal way. In order for the processing to be considered legal, legal requirements are required
at least one of the conditions of Article 6 (1) is met.
The provision of health care is one such task of general
interest referred to in Article 6 (1). e.
In health care, the legal bases can also be legal

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

updated.

1 4 (31)

The Data Inspectorate

DI-2019-3843

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

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

6.2, maintain or introduce more specific provisions for adaptation

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

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

and other measures to ensure legal and fair treatment. But

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

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

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

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

specific provision to adapt the application of the provisions of

the Data Protection Regulation. Union law or the national law of the Member States

law must fulfill an objective of general interest and be proportionate to it

legitimate goals pursued.

Article 9 states that the treatment of specific categories of

personal data (so-called sensitive personal data) is generally prohibited.

Sensitive personal data includes data on health. In Article 9.2

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

Article 9 (2) (h) states that the processing of sensitive personal data may be repeated

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

the provision of health care on the basis of Union law or

national law of the Member States or in accordance with agreements with professionals in

the field of health and provided that the conditions and protective measures provided for in

referred to in paragraph 3 are met. Article 9 (3) requires a regulated duty of confidentiality.

This means that both the legal bases of general interest,

exercise of authority and legal obligation in the treatment of the vulnerable

personal data under the exemption in Article 9 (2). h need

supplementary rules.

Supplementary national regulations

In the case of Sweden, both the basis for the treatment and those

special conditions for the processing of personal data in the field of health and

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

the Patient Data Ordinance (2008: 360). I 1 kap. Section 4 of the Patient Data Act states that

the law complements the data protection regulation.

The purpose of the Patient Data Act is to provide information in health and

healthcare must be organized so that it meets patient safety and



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

personal data shall be designed and otherwise processed so that patients and

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

personal data is handled and stored so that unauthorized persons do not have access to it

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

The supplementary provisions in the Patient Data Act aim to:

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

thus through the regulation made a balance in terms of how

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

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

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

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

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

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

personal data in health care.

National provisions that supplement the requirements of the Data Protection Regulation

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

2016: 40.

Requirement to do needs and risk analysis

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

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

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

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

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

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

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

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

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

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

eligibility assignments based on analyzes of which details are different

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

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

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

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

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

may require special risk assessments.



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

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

categories of healthcare professionals for electronic access to data in

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

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

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

dissemination of medical records within an

not accepted.

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

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

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

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

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

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

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

limited to individuals.

Internal secrecy

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

regulates how privacy protection is to be handled within a care provider's business

and in particular employees' opportunities to prepare for access to

personal data that is electronically available in a healthcare provider

organisation.

It appears from ch. Section 2 of the Patient Data Act, that the care provider shall decide

conditions for granting access to such data

patients who are fully or partially automated. Such authorization shall

limited to what is needed for the individual to be able to fulfill theirs

tasks in health care.

According to ch. 4 § 2 HSLF-FS 2016: 40, the care provider shall be responsible for each

users are assigned an individual privilege to access

personal data. The caregiver's decision on the allocation of eligibility shall

preceded by a needs and risk analysis.

Coherent record keeping

The provisions in ch. 6 the Patient Data Act concerns cohesive record keeping,

which means that a care provider - under the conditions specified in § 2 of the same

chapter - may have direct access to personal data processed by others

caregivers for purposes related to care documentation. The access to

information is provided by a healthcare provider making the information about a patient

which the care provider registers if the patient is available to other care providers

who participate in the coherent record keeping (see Bill 2007/08: 126 p. 247).



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

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

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

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

record keeping.

Documentation of access (logs)

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

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

automatically documented and systematically checked.

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

1. the documentation of the access (logs) states which

measures taken with information on a patient,

2. it appears from the logs at which care unit or care process

measures have been taken,

3. the logs indicate the time at which the measures were taken;

4. the identity of the user and the patient is stated in the logs.

The Data Inspectorate's assessment

Responsibility of the data controller for security

As previously described, Article 24 (1) of the Data Protection Regulation provides:

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement is partly to ensure that

the processing of personal data is carried out in accordance with

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

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

the Data Protection Regulation.

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

5.1 (f) and Article 32 of the Data Protection Regulation.

Article 32 (1) states that the appropriate measures shall be both technical and

organizational and they must ensure a level of security appropriate in

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

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

the risks to the data subjects' rights and freedoms and assess



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

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

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

thus the significance of what personal data is processed, how many

data, it is a question of how many people process the data, etc.

The health service has a great need for information in its operations. The

It is therefore natural that the possibilities of digitalisation are utilized as much as

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

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

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

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

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

safety is affected by the extent of the treatment.

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

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

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

people and the data may over time be processed by very

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

personal data controller.

The data processed must be protected from outside actors as well

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

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

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

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

be able to know what is an unauthorized access it must

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

Needs and risk analysis

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

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

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

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

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

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

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

with an overly allotment of access to personal data

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



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

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

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

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

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

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

that it is a question of protected personal data, publicly known persons or

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

the risk assessment. The preparatory work for the Patient Data Act shows that the more

comprehensive an information system is, the greater the variety

eligibility levels must exist. (Prop. 2007/08: 126 p. 149). It is thus

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

authorization 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 give one

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

updated.

In summary, the regulation requires that the risk analysis identify

- 

different categories of data (eg health data),

- 

categories of data subjects (eg vulnerable natural persons and

children), or

- 

the scope (eg number of personal data and registered)

- 

negative consequences for data subjects (eg damages,

significant social or economic disadvantage, deprivation of rights

and freedoms),

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

Processing of personal data. This applies to both internal secrecy

as in coherent record keeping.

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

based on whether there is protected personal data that is

classified, information on public figures, information from

certain clinics or medical specialties (Bill 2007/08: 126 p. 148149).



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

the risk to the data subjects' rights and freedoms is and in any case determined

whether it is a risk or a high risk (recital 76).

It is thus through the needs and risk analysis that it

personal data controller finds out who needs access, which

information the accessibility shall include, at what times and at what

context access is needed, while analyzing the risks to it

the freedoms and rights of the individual that the treatment may lead to. The result should

then lead to the technical and organizational measures needed to

ensure that no access other than that of need and

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

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

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

be able to assign their users a correct authorization. The

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

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

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

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

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

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

required.

Region Östergötland's process for needs and risk analysis

When the Data Inspectorate has requested a documented needs and

risk analysis, the Regional Board has referred to three documents; Assessment of

eligibility allocation after performed needs and risk analysis, Needs and

risk analysis of authorizations and Management of authorizations. The Data Inspectorate

can state that there are instructions and guidelines that concern the needs and risk analysis at user level, which to some extent

talks about how to go

prepare for the performance of a needs and risk analysis at user level and

that a needs and risk analysis at user level must be done before allocation of

permissions occur in the system. However, the Data Inspectorate can further establish

that the information in these documents only accounts at an overall level

for how to proceed before performing this analysis and that

there is no essential information for a needs and risk analysis to be able to

performed correctly. There is a lack of e.g. an analysis of what is needed

information different users have and an analysis of the risks involved

access to, for example, certain categories of data or different types of

activities that contain sensitive information. Furthermore, the final one is missing



analysis that emerges when the need for data is weighed against the risk that

access to the data may entail. There are also no analyzes of

the business, the processes and an identified need for information in different

staff categories available from 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 so - either

within the framework of internal secrecy or within it

coherent record keeping. The Regional Board considers the document

Assessment of eligibility allocation after performing needs and risk analysis is one

needs and risk analysis and “forms a basis for the risk analysis that is

completed and that completed form relating to the ordering of authorizations

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

needs and risk which also refers to coherent record keeping ”.

The Data Inspectorate can state that this document is not an actual one

needs and risk analysis.

Authorization allocation is in itself an important organizational measure to

ensure correct access to personal data. A needs inventory constitutes

a step 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 securing measures to manage the risks of unjustified

spread.

Due to the above, the Data Inspectorate can state that

there is no 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 secrecy,

partly within the framework of the coherent record keeping according to 4 resp. Chapter 6

the Patient Data Act. The documents that have been reported do not meet the requirements

which is placed on a needs and risk analysis. As a result, the Regional Board has not

also been able to show that assigned privileges are correct. This means one

significant risk of unauthorized access to care and patient data.

The person responsible for personal data is responsible for following the basics

the principles of data minimization and appropriate security in accordance with Article 5, 24

and 32 of the Data Protection Regulation and has to show that the processing of

the personal data is performed in accordance with the Data Protection Regulation.

As the person responsible for personal data, the Regional Board has not complied

liability under Article 5 (2) of the Data Protection Regulation by:

be able to show that the regulations are complied with.



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

The Regional Board during the review on April 10, 2019 has considered

personal data in breach of Article 5 (1) (f) and (2), Article 24 (1) and Article 32 (1)

0ch 32.2 of the Data Protection Regulation by failing to comply with the requirement that

carry out a needs and risk analysis before the allocation of authorizations takes place in

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

the Patient Data Act and Chapter 4 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 show that the processing of personal data has

a security that is appropriate in relation to the risks.

Authorization of access to personal data about patients

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

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

access to personal data about patients may be limited to

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

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

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

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

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

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

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

unauthorized dissemination of journal information within a business and should as

such is not accepted. "

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

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

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

responsible for personal data finds out who

need access, what information the access should include, at what times

and in what contexts access is needed, while analyzing which ones

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

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

is needed to ensure that the allocation does not provide further access possibilities

than that shown by the needs and risk analysis is justified. An important

organizational action is to provide guidance to those who have the authority to

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

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

allocation of competence in each individual case.



It appears that in Cosmic there are four modules that contain

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

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

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

users have been granted basic access to the module Care Documentation, 6 102

users have been granted basic access to the Pharmaceutical module, 5,956
users have been assigned basic access to the Care Administration module and 5
848 users have been assigned basic access to the Referral module. This means
that a majority of users have been granted access to the four
the modules in Cosmic.
With regard to restrictions in Cosmic, the Regional Board has exclusively
reported on the personal data contained under "All notes" in
the module "Care documentation". The Regional Board has stated that there are three
types of classified information and that users have the opportunity to
confidentiality class information regarding two of these three confidentiality classes.
Regarding the confidentiality class "No access with logging", this takes place
classification of the caregiver. There are two units at the University Hospital in
Linköping whose information has been given this confidentiality class. The Data Inspectorate
notes that there has been a real restriction on users' access to them
case.
Regarding the other two secrecy classes, “Create journal reference with
logging ”and“ Warning with logging ”, are the personal data that has been stored
with this "confidentiality" still electronically accessible through active elections.
By the user clicking in the box for consent or emergency access can
he still has access to all personal data, which means that everyone
users who make these active choices can access patients' information and
not just the users who have a need.
Of the preparatory work for the Patient Data Act, Bill. 2007/08: 126, p. 149, it appears that
the purpose of the provision on access restriction in ch. 4 § 2
The Patient Data Act is to imprint the obligation on the responsible care provider
to make active and individual eligibility assignments based on analyzes of

which details different staff categories and different types

businesses need. The preparatory work shows that information should also

stored in different layers so that more sensitive tasks require active choices or otherwise

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



That the Regional Board uses the above active choices is one

integrity enhancement measure, but does not imply that these active choices constitute a

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

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

that the individual should be able to fulfill his tasks in health and

healthcare, ie. only those in need of the data shall have access, and

no such restriction has taken place. The Data Inspectorate also questions

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

classify the information, and not the Regional Board itself.

The Regional Board has exclusively reported on the personal data that is available

under "All notes" in the module "Care documentation" regarding

the possibility for the user to classify information confidentially. Otherwise have

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

confidentiality classes in respect of other personal data or in other modules.

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

Cosmic has access to the module "Medicines - Basic", even if it exists

possibility to restrict access to the data in this module.

Because different users have different tasks within different

workspaces, users need access to the data in Cosmic

limited to reflect this. The Regional Board has, apart from those
information that has been given the confidentiality class "No logging access", no
restricted users 'permissions to access patients'
personal data in the record system, whether within the framework of the internal
secrecy or within the framework of the unified record keeping in
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 permissions of the users have thus not been limited in such a way that
the provisions of the Patient Data Act require and the Regional Board has not, i
in accordance with Article 32, have taken sufficient technical measures to:
restrict users' access to personal data in
the journal systems to only what is needed for the user to be able to
perform their duties. This means the allocation of privileges
has been too extensive, general and implemented for one for the personal
the integrity of the intervention and thereby been disproportionate in
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
confidentiality, which covers 516,416 patients, partly within its framework
integrated record keeping, which includes 838,093 patients. The number
users are 7,014 and the number of users who have gained access to
the data in the various modules are between 5,848 - 6,221.

It appears that the Regional Board has not limited health and

access to healthcare professionals and medical secretaries

patient information either in the context of internal confidentiality or

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

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

The Regional Board during the review on April 10, 2019 has considered

personal data in breach of Article 5 (1) (f) and (2), Article 24 (1) and Article 32 (1)

0ch 32.2 in the Data Protection Ordinance in that the Regional Board has not

restricted users' permissions to access the Cosmic journal system

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

tasks in health care according to ch. 4 § 2 and ch. 6 § 7

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

The Regional Board has not taken measures to ensure and

be able to show appropriate security for personal data.

Documentation of access (logs)

The Data Inspectorate can state that it appears from the logs in Cosmic

information about the specific patient, which user has opened

the journal, measures that have been 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.

The Data Inspectorate 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 in accordance with Article 32 of the Data Protection Regulation;

Choice of intervention

Legal regulation

If there has been a violation of the Data Protection Regulation

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



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

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

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

specific period.

Article 58 (2) (i) and Article 83 (2) of the Data Protection Regulation state that:

The Data Inspectorate has the authority to impose administrative penalty fees

in accordance with Article 83. Furthermore, depending on the circumstances of

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

instead of the other measures in Article 58 (2).

For Article 83 (7), authorities may receive national data protection regulations

rules state that administrative sanctions may be imposed on authorities.

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

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

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

or 83.5 of the Data Protection Regulation.

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

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

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

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

in the case of a minor infringement, the supervisory authority may, according to reasons

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

penalty fee.

Order

The health service has a great need for information in its operations. The

It is therefore natural that the possibilities of digitalisation are utilized as much as

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

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

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

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

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

safety is affected by the extent of the treatment.

In health care, this means a great responsibility for it

personal data controller to protect the data from unauthorized access,

among other things by having an authorization allocation that is even more

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

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



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

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

this analysis must then be restricted to the individual executive.

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

hand that changes in the individual executive's duties

reason for it.

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

risk analysis, something that is directly prescribed in ch. 2 § HLSF-FS 2016: 40. The
means that the Regional Board has had no basis for assessing whether
the need or risk in granting eligibility. It has also led to that
access for employees has not been limited to what is needed to
the individual must be able to fulfill his duties in health and
healthcare. This applies to access within the internal secrecy according to ch.
the Patient Data Act as the cohesive record keeping according to ch.
the Patient Data Act.

The Data Inspectorate therefore submits in accordance with Article 58 (2) (d) i
the Data Protection Ordinance The Regional Board to implement and document
required needs and risk analysis for the journal system Cosmic and that
then, based on the needs and risk analysis, assign each user
individual authority for access to personal data to only what
needed for the individual to be able to fulfill their 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 Ordinance, Chapter 4 § 2 and ch. 6 § 7
the Patient Data Act and Chapter 4 2 § HSLF-FS 2016: 40.

Penalty fee

The Data Inspectorate can state that the violations concern the Regional Board
obligation to provide protection of personal data with appropriate security measures
pursuant to Article 32 of the Data Protection Regulation.

In this case, it is a matter of large collections of data with sensitive
personal data and extensive powers. The caregiver needs to be involved
necessity to have a comprehensive processing of data on the health of individuals.
However, it must not be unrestricted but should be based on what individual
employees need to be able to perform their tasks. The Data Inspectorate

notes that this is information that includes direct identification of

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

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



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

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

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

responsibility to ensure patients' right to adequate protection for their

personal data.

Additional aggravating circumstances are the treatment of

patient information in the main medical record system belongs to the core of a healthcare provider

activities and treatment include many patients and the possibility of

access refers to a large proportion of employees. In this case, it is 516,416

unique patients within the framework of internal confidentiality, and 794 626 unique

patients in the context of coherent record keeping. There is

only two devices where the data is not accessible to users outside

these devices.

It has further emerged that the Regional Board has not rectified this before

the injunction from the Swedish Data Inspectorate, dated 27 March 2015, there

The Regional Board was instructed to produce a documented needs and

risk analysis that met the then requirement ch. 2 § 6 § second paragraph

second sentence SOSFS 2008: 14, which corresponds to the current provision in 4

Cape. 2 § HSLF-FS 2016: 40. This is, according to Article 83 (2) (e)

the Data Protection Regulation, to be considered as an additional complication

circumstance.

The Data Inspectorate states that the shortcomings that have now been established have been known to the Regional Board for several years, which means that the action intentionally and thus is considered more serious.

In determining the seriousness of the infringements, it can also be stated that the infringements also concern Article 5, which is said to be one of the more serious infringements which may give rise to a higher penalty under Article 83 (5).

Taken together, these factors mean that the infringements in question are not to judge as minor violations but the violations should lead to one administrative penalty fee.

The Data Inspectorate considers that these violations are closely related to each other. That assessment is based on the need and risk analysis form the basis for the allocation of the authorizations. The Data Inspectorate therefore considers that these infringements are so closely linked that they constitute interconnected data processing within the meaning of Article 83 (3) (i)



the Data Protection Regulation. The Data Inspectorate therefore decides on a joint penalty fee for these infringements.

The administrative penalty fee shall be effective, proportionate and deterrent. This means that the amount must be determined so that it the administrative penalty fee leads to correction, that it provides a preventive effect and that it is also proportional in relation to both current violations as to the ability of the supervised entity to pay.

The maximum amount for the penalty fee in this case is SEK 10 million

according to ch. 6 Section 2 of the Act (2018: 218) with supplementary provisions to the EU

data protection regulation.

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

shall be effective, proportionate and dissuasive

The Data Inspectorate the administrative sanction fee for the Regional Board

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

_____

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

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

The case is handled by Hans-Olof Lindblom, General Counsel, 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 a penalty fee

Copy for information to:

Data Protection Officer

3 0 (31)

The Data Inspectorate

DI-2019-3843

How to appeal

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

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

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

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

the Data Inspectorate forwards it to the Administrative Court in Stockholm

examination.

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

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

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