Decision

Diarienr

2020-12-02

DI-2019-3844

Aleris Sjukvård AB

c / o Aleris Specialist care Sabbatsberg

Box 6401

113 82 Stockholm

Stockholm County

Supervision under the Data Protection Regulation and

Patient Data Act- needs and risk analysis and

questions about access in journal systems

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

The Data Inspectorate

DI-2019-3844

The Data Inspectorate's decision

During a review on April 8, 2019, the Data Inspectorate has established that Aleris Sjukvård AB processes personal data in violation of Article 5 (1) f and 5.2 and Article 32 (1) and (2) of the Data Protection Regulation1 by

1.

Aleris Sjukvård AB has not carried out a needs and risk analysis before the allocation of permissions takes place in the journal system TakeCare, i in accordance with ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act (2008: 355) and ch. 4 Section 2 The National Board of Health and Welfare's regulations and general advice on record keeping and processing of personal data in health and healthcare (HSLF-FS 2016: 40). This means that Aleris Sjukvård AB have 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.

2. Aleris Sjukvård AB does not limit users' permissions for access to the TakeCare medical record system for what is only needed for that the user shall be able to fulfill his tasks in health and medical care according to ch. § 2 and ch. 6 Section 7 of the Patient

Data Act and 4

Cape. 2 § HSLF-FS 2016: 40. This means that Aleris Sjukvård AB does not have

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

security of personal data.

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

the Data Protection Ordinance that Aleris Sjukvård AB, for violation of

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

shall pay an administrative penalty fee of 15,000,000 (fifteen

million).

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

data protection ordinance Aleris Sjukvård AB to implement and document

required needs and risk analysis for the TakeCare medical record system and that

then, based on the needs and risk analysis, assign each user

1

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

on the protection of individuals with regard to the processing of personal data and on that

free flow of such data and repealing Directive 95/46 / EC (General

Data Protection Regulation).

individual access to personal data restricted to

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

duties in health care, in accordance with Article 5 (1) (f) and

Article 32 (1) and (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.

Report on the supervisory matter

The Data Inspectorate's inspection began with an inspection letter on 22 March 2019 and has taken place both in writing and through on-site inspection on 8 April 2019. The audit has been intended to control whether Aleris Sjukvård AB's (hereinafter referred to as Aleris) decision on the allocation of authorizations has been preceded by a need and risk analysis. The supervision has also included how Aleris has granted authorizations for access to the TakeCare master journal system, and which access opportunities the granted privileges provide within both the framework of the internal secrecy according to ch. the Patient Data Act, as the cohesive one record keeping according to ch. 6 the Patient Data Act. In addition to this has The Data Inspectorate examined which documentation of access (logs) is in the journal system.

The Data Inspectorate has only examined the user's access to the journal system, i.e. what care documentation the user can actually take part of and read. The supervision has not included which functions were included in the competence, ie. what the user can actually do in the journal system (eg issuing prescriptions, writing referrals, etc.).

The inspection is one of several inspections within the framework of a self-initiated supervisory project at the Swedish Data Inspectorate, where i.a. Karolinska The university hospital has been included. Due to what has emerged about Aleri's view on the technical possibilities to limit readability for its TakeCare users, Aleris was specifically asked to do so comment on an opinion from Karolinska University Hospital, which also uses TakeCare, where the technical possibilities regarding TakeCare was described.

What has emerged in the case

Aleris has essentially stated the following.

The responsibility for personal data

Aleris is the care provider and personal data manager.

The business

Aleri's ownership structure has changed after the Data Inspectorate's inspection

initiated. Aleris 'new ownership structure is shown in Aleris' supplement from 16

November 2020. The supplement states, among other things, the following.

Aleris has been part of the newly formed Group Parent Company since October 1, 2019,

Aleris Group AB (corporate identity number 559210-7550), and is a subsidiary of Aleris

Healthcare AB (org.nr. 556598–6782). Aleris Group AB is owned by Triton.

Group sales for Aleris Group AB amounted to SEK 1,215,385,000

between October 1, 2019 and December 31, 2019. Since Aleris Group

AB was formed in connection with the change of ownership when Aleris Healthcare AB joined

subsidiaries were acquired, only turnover figures are available for this

period.

The annual turnover for Aleris Healthcare AB amounted to SEK 30,223,866

during 2019.

Journal system

Aleris has been using TakeCare as its main medical record system since 28 May 2012

for internal secrecy and within the framework of cohesion

record keeping.

Federation Collaboration TakeCare (FSTC) is the customer of the medical record system

TakeCare and CompuGroup Medical (CGM) are suppliers of the medical record system

and is responsible for the functions that the system has to control permissions.

All functions in the journal system are created by CGM, but it is Aleris who

chooses which functions a certain category of staff should have access to among

the functions that are entered. Aleris has no technical possibilities to do

changes in TakeCare because Aleris has no control over

the journal system. Aleris is only a user of the system.

Aleris has not been able to make any demands on CGM in the procurement of

the journal system. The company has, for example, pointed out that there have been problems

with the record system consisting of, as far as the allocation of competences is concerned, that

the system cannot separate read and print permissions for a read function.

CGM has not been interested in changing this despite comments from

Aleris.

It is FSTC that can order changes to the functions and that is then

up to CGM if they want to make the changes or not. Aleris has one

representative in FSTC who can express Aleri's wishes. However, Aleris has not

received some hearing for the company's views.

Number of patients and employees

Aleris had 796,350 unique patients in TakeCare as of May 20, 2019. How

however, many of those who died could not be retrieved.

In May 2019, there were 1,058 active users, 807 active accounts and 63

units in the journal system TakeCare. The number of active users (ie employees
and consultants who may have access to TakeCare) have been calculated by
calculate the number of active AD accounts at relevant cost centers.

Internal secrecy

Aleris has essentially stated the following.

Needs and risk analysis

Aleris has stated that needs and risk analyzes aimed at TakeCare are performed
by a designated risk analysis team for the purpose of reviewing the applicable authorization allocation
and possibly determine new conditions for granting eligibility. Permissions
is always limited to what is needed for the employee to be able to perform
their work and contribute to safe care. The need versus the risk of improperness
access is always weighed against each other before permissions are granted. General
authorization profiles are available, specific authorizations are assigned if necessary. The
later examined in particular in the subsequent analysis of the designated risk analysis team. What
What is especially considered are the risks that can arise if an employee has
too broad eligibility versus too low eligibility and thus not access to
relevant patient information. The result from the needs and risk analysis is
then the basis for selecting the authorization profile used in the assignment
of competencies within Aleris.

Eligibility for TakeCare is ordered by the responsible manager, as stated in
the document, “TakeCare Authorization Management”. The document also states
that the competence is personal and that its scope is based on

the user's professional role and organizational domicile. Furthermore, it appears that the care provider must ensure that the authority for access to patient data limited to what a user needs to be able to perform their tasks in health care.

Aleris has a document called "Needs and Risk Analysis-TakeCare". The document has looked like it does today since May 28, 2012 when TakeCare was introduced and applies both to internal secrecy and within its framework coherent record keeping. The document shows the different profiles, so-called authority groups. The document shows, among other things the reading rights and the writing rights for each authority group.

All profiles except technicians have been granted read access to the data in TakeCare. The eligibility for each group has been justified. The doctors are going examples be able to perform their duties and are responsible for patient information, while the system administrator must be able to troubleshoot, manage and set up users, systems and local administrators.

Under the heading "Risk of restricted access" it is stated that the user "can not perform their duties fully ". This justification is stated for all profiles (except for the local administrators where the motivation is “Can not manage permissions and implement corrective actions "). During The heading “Risk of extensive access” states, among other things, that “There is one risk of disclosure of patient information '. Similar justification is given for everyone profiles.

Authorization of access to personal data about patients

Aleris has stated that it is the system administrator who has the highest the level of competence, ie full authorization, in TakeCare. The local the administrator has access to his own device and is the one who assigns

permissions within the device. What privileges an administrator imposes

a user depends on the business to which the user belongs and on

the user's tasks. All users get the “minimum they should have

to cope ”in terms of accessibility. Access can, however

expanded if necessary. There are basic profiles for, for example, assistant nurses,

who are given the qualifications needed to carry out their duties

tasks. If the manager deems that the assistant nurses need one

extended privileges, local administrators ensure that privileges

"Hangs up" the basic profile. If the extended authorization is not needed, it can be taken

away from the basic profile.

Aleris has stated that all accounts within Aleris are individual and that

the authorizations are assigned on the basis of the document, “Needs and risk analysisTakeCare”. As previously mentioned, it

appears from the document that everyone

professional profiles in addition to technicians have been granted permission to read the data in

TakeCare.

However, Aleris has stated that all users have different read permissions in

the journal system based on which system functions they have access to

Aleris. According to Aleris, it is possible to steer away access opportunities to TakeCare

by giving different staff access to different functions. Each

staff category only gets access to the functions they need for

to be able to perform their work. Technicians, for example, have limited qualifications

depending on what they are going to do in the system. They only get reading permission if they

need it in their work. Another example concerns users who only

will be at the checkout and thus do not need a reading license.

There are no staff who only have the task of managing the cash register

the current situation.

By choosing different functions for different users, a difference is made in

what different users can do in the system, e.g. as regards verify, sign,

etc. In total, there are 640 different system functions that you can choose to provide

authority to. Among these features, Aleris has selected the features that

different staff categories need to have access to in order to operate safely

patient work. The document "Profiles and permissions" shows the different ones

permissions that each category of staff has been assigned in TakeCare, e.g.

dictate audio files, read activities, sign, read emergency information, read journal text,

vidimering, read referral, administer drug prescription, read scanned

documents and approve care sessions. The document states, among other things

that all profiles ie. doctors, nurses, assistant nurses,

paramedics, secretaries, "administrative", students and "Receptionist

Rehab "has the authority to" read journal text "and that everyone except

"Receptionist Rehab" is authorized to "read scanned documents" in

TakeCare. It also appears that only doctors are authorized to “read

emergency tasks ”and that all profiles except the assistant nurse and

"Administrative" can "read diagnoses" in TakeCare.

Aleris has stated that the starting point is that one user on one device only

has read access to the patient records available on the device. One

users who need to read journal entries from another device must

make an active choice in the system. By active choices is meant that the user is allowed to do a number of "clicks" and select the current device (this function is called journal filter). Authorization to be able to use the journal filter is given to them users who need this to be able to perform their work.

The user can never accidentally read one patient record from another unit.

Aleris has stated that there are features in TakeCare for a caregiver should be able to "isolate" one care unit and thereby "shut out" others caregivers 'and care units' access possibilities to the unit's care documentation, so-called protected units. However, Aleris does not operate any business that requires protected devices and has therefore not used of this function.

Coherent record keeping

Aleris has essentially stated the following.

Needs and risk analysis

The document "Needs and risk analysis - TakeCare" also applies to the system for coherent record keeping.

Authorization of access to personal data about patients

The allocation of authority takes place in the same way as within the framework of the internal secrecy.

Within the framework of coherent record keeping in TakeCare, users can take part of all care documentation with other care providers included in the system.

The user can initially see if a patient is current with other care providers, but not which. To be able to see who these caregivers are, the user must

click on in the system, ie. make active choices. The user must then

click in the box "consent" or "emergency access" to access it

specific caregiver records.

Aleris has stated the following due to Karolinska

The University Hospital in a statement has stated that there are opportunities to

restrict access in TakeCare.

There is a function to "isolate" a care unit and thereby close

access to other care providers and care units (so-called

protected devices). A care provider can thus from a technical perspective

restrict other care providers' access to their own care documentation.

However, Aleris has assessed that the company does not conduct any business as

need to be blocked and that it is more patient safe to let the patient information

at Aleris units be available to other care providers. According to Aleris, it is

in addition, not allowed to implement such restrictions if one

caregivers use the TakeCare medical record system and at the same time are part of

coherent record keeping. This following a decision from the Stockholm Region. The

means that all users of Aleris have access to all patient data

at the other care providers in TakeCare, except when patients have requested to

get their information blocked (a so-called caregiver block).

According to Aleris, from a patient safety perspective, this is not practically possible

to opt out of individual care providers' access to their own care documentation

in TakeCare (except for protected devices). Either is the caregiver

included in the system for coherent record keeping or not. It is not possible to restrict access for competent persons to the information of other care providers and at the same time in a meaningful way participate in coherent record keeping. According to Aleris, it is not possible to determine in advance which data are in one certain cases may be important for patient-safe care. Aleris has therefore decided not to actively block other caregivers' records. However, such as mentioned, a caregiver himself blocks other caregivers' access to TakeCare there these have made the assessment that their patients' medical records should not be available to other caregivers. These devices are marked in TakeCare with an asterisk. In this way, a selection of care units has already been made Aleri's staff do not have access to.

Documentation of access (logs)

Aleri's log documentation states, among other things, the following: the user's and patient's identity, care unit, date, time, information to the user has documented in the journal during the last 18 months as well as information that the patient has had contact with the care unit during the last 18 months.

Aleris has the ability to perform targeted log checks. That means Aleris can see exactly what a user has done in the system. About the patient or Aleris suspects data breaches, Aleris can also perform an in-depth log check.

Also all activities that take place within the framework of coherent record keeping logged in the system. It also means that all active selections are logged in the system. If

the user, for example, selected "consent" or "emergency access", to be able to take

part of a patient's information to another care provider, this will be

appear from the log documentation.

Aleri's opinion on the Data Inspectorate's letter

Aleris has in comments on the letter Final communication before decision as

received by the Swedish Data Inspectorate on 20 March 2020 stated, among other things, the following.

The Data Inspectorate should consider the figures for the economic unit where they

The alleged shortcomings have taken place, ie Aleris Sjukvård AB.

Aleris has actively worked to continuously strengthen the interior and exterior

confidentiality, including the functionality of TakeCare. When Aleris took over

adequate measures to strengthen, through FSTC, the integrity of TakeCare

actual deficiencies in TakeCare should not be considered to be Aleris' fault.

Justification of decision

Applicable rules

The Data Protection Regulation is the primary source of law

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

is the primary legal regulation in the processing of personal data. This

also applies to health care.

The basic principles for the processing of personal data are set out in

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

security pursuant to Article 5 (1) (f), which states that personal data shall be processed

in a way that ensures appropriate security for personal data,

including protection against unauthorized or unauthorized treatment and against loss;

destruction or damage by accident, using appropriate

technical or organizational measures.

Article 5 (2) states the so-called liability, ie. that it

“Personal data controllers must be responsible for and be able to show that they

the basic principles of paragraph 1 are complied with ".

Article 24 deals with the responsibility of the controller. Of Article 24 (1)

it appears that the person responsible for personal data is responsible for implementing appropriate

technical and organizational measures to ensure and be able to demonstrate that

the processing is performed in accordance with the Data Protection Regulation. The measures shall

carried out taking into account the nature, scope, context of the treatment

and purposes and the risks, of varying degrees of probability and severity, for

freedoms and rights of natural persons. The measures must be reviewed and updated

if necessary.

Article 32 regulates the security of the processing. According to paragraph 1

the personal data controller and the personal data assistant shall take into account

of the latest developments, implementation costs and treatment

nature, scope, context and purpose as well as the risks, of varying

probability and seriousness, for the rights and freedoms of natural persons shall

the personal data controller and the personal data assistant take appropriate

technical and organizational measures to ensure a level of security

which is appropriate in relation to the risk (…). According to paragraph 2, at

the assessment of the appropriate level of safety takes special account of the risks involved

the treatment entails, in particular from accidental or unlawful destruction,

loss or alteration or to unauthorized disclosure of or unauthorized access to

the personal data transferred, stored or otherwise processed.

Recital 75 states that in assessing the risk to natural persons

rights and freedoms, various factors must be taken into account. Among other things mentioned

personal data covered by professional secrecy, health data or

sexual life, if the processing of personal data concerning vulnerable physical persons takes place

persons, especially children, or if the treatment involves a large number

personal data and applies to a large number of registered persons.

Furthermore, it follows from recital 76 that the likelihood and seriousness of the risk for it

data subjects' rights and freedoms should be determined on the basis of processing

nature, scope, context and purpose. The risk should be evaluated on

on the basis of an objective assessment, which determines whether

the data processing involves a risk or a high risk.

Recitals 39 and 83 also contain writings that provide guidance on it

the meaning of the Data Protection Regulation's requirements for security in

Processing of personal data.

The Data Protection Regulation and the relationship with complementary national

provisions

According to Article 5 (1). a of the Data Protection Regulation, the personal data shall

treated in a lawful manner. In order for the treatment to be considered legal, it is required

legal basis by at least one of the conditions of Article 6 (1) being met.

The provision of health care is one such task of general

interest referred to in Article 6 (1) (e).

In health care, the legal bases can also be legal

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

updated.

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

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

6.2, maintain or introduce more specific provisions for adaptation

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

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

and other measures to ensure legal and fair treatment. But

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

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

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

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

specific provisions to adapt the application of the provisions of

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

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

legitimate goals pursued.

Article 9 states that the treatment of specific categories of

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

personal data includes data on health. Article 9 (2) states

except when sensitive personal data may still be processed.

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

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

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

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

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

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

This means that both the legal bases of general interest,

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

personal data under the derogation in Article 9 (2) (h)

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, see chap. Section 1 of the Patient Data Act.

National provisions that supplement the requirements of the Data Protection Regulation security can be found in Chapters 4 and 6. the Patient Data Act and Chapters 3 and 4 HSLF-FS 2016: 40.

Requirement to make a 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 information 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.

Of ch. 4 § 2 HSLF-FS 2016: 40 follows that the care provider shall be responsible for each

users are assigned an individual privilege to access

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

preceded by a needs and risk analysis.

Coherent record keeping

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

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

chapter of that law - may have direct access to personal data that is processed

by other care providers 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

which participates in the cohesive record keeping system (see Bill 2007/08: 126

p. 247).

Of ch. 6 Section 7 of the Patient Data Act follows that the provisions in Chapter 4 Sections 2 and 3 also apply to authorization

allocation and access control at cohesion

record keeping. The requirement that the care provider must perform a needs and risk analysis

before the allocation of permissions in the system takes place, thus also applies in systems

for coherent record keeping.

Documentation of access (logs)

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

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

automatically documented and systematically checked.

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

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

measures taken with information on a patient,

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

measures have been taken,

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

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

The Data Inspectorate's assessment

Responsibility of the data controller for security

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

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement is partly to ensure that

the processing of personal data is carried out in accordance with

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

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

the Data Protection Regulation.

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

5.1 f and 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.
It is therefore natural that the possibilities of digitalisation are utilized so 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 and the data 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 that the data over time may be processed by very

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

personal data controller.

The data processed must be protected from outside actors as well

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

It should be noted that Article 32 (2) states that the controller, at

assessment of the appropriate level of safety, in particular taking into account the risks of

unintentional or unlawful destruction, loss or unauthorized disclosure or

unauthorized access. To be able to know what is an unauthorized access must

the data controller must be clear about what is an authorized access.

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

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 (Bill 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.

In summary, the regulation requires that the risk analysis identify

-

different categories of 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 based on

the nature, scope, context and purpose of the treatment (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.

Aleris has stated that the authorizations are granted on the basis of the document, "Needs and risk analysis-TakeCare". The document states that all

authorization profiles in addition to technicians have been assigned permission to read in the system,

and that the risk with limited access is that the user can not perform their

tasks in full. This justification is stated for all users.

It is further stated that the only risk in the event of extensive access is to the user

sees information that he / she does not have the right to see which may involve disclosure

of patient information. Similar justification is given for all profiles. The

means that Aleris makes the same assessment for all profiles regardless

the user's task and needs.

The Data Inspectorate can state that the document, "Needs and risk analysisTakeCare" does not contain any analysis of the different profiles' needs for

access to patients' data. Aleris has only stated what respectively

profile "must be able to perform" in the journal system and thus not analyzed which

information such as the question of or what the needs look like in the various

the business components and for different professional roles. The document also lacks one

analysis of the risks to the individual's freedoms and rights as an excessive

eligibility may entail. The needs and risk analysis must be done in a strategic manner

level that should provide a competency structure that is adapted to the business.

The information in the document "Needs and risk analysis - TakeCare" is too

deficient in relation to the information required for a correct

needs and risk analysis must be able to be performed. As stated above, in a

needs and risk analysis both the needs and the risks are 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 individual's integrity exist as well

organizational as well as individual level.

In its analysis, Aleris has not taken into account the negative consequences for

registered, different categories of data, categories of registered or

the extent of the number of personal data and data subjects affects the risk of

the rights and freedoms of natural persons in the treatment of Aleris by

personal data in TakeCare. There are also no special risk assessments

based on whether there is, for example, protected personal data that is

classified, information on public figures, information from

certain clinics or medical specialties or other factors such as

requires special protective measures. There is also no assessment of how

probable and serious risk to the data subjects' rights and freedoms

is considered to be.

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

the document “Needs and risk analysis- TakeCare” does not meet the requirements

put on a needs and risk analysis and that Aleris has not been able to show that

the company has carried out a needs and risk analysis within the meaning of 4

Cape. § 2 HSLF-FS 2016: 40, neither within the framework of internal secrecy

according to ch. 4 the Patient Data Act or within the framework of the cohesive

record keeping according to ch. 6 Section 7 of the Patient Data Act. That means Aleris does not

have taken appropriate organizational measures in accordance with Article 5 (1) (f) and

Article 32 (1) and (2) in order to ensure and, in accordance with Article 5 (2),

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

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

access to personal data about patients may be limited to

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

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

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

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

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

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

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

unauthorized dissemination of journal information within a business and should as

such is not accepted. "

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

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

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

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

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

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

analyzes the risks to the individual's freedoms and rights

the treatment can lead to. The result should then lead to the technical and organizational measures needed to ensure no allocation of eligibility provides further access opportunities than the one that needs and the risk analysis shows is justified. An important organizational measure is to provide instruction to those who have the authority to assign permissions on how this should go to and what should be considered so that it, with the needs and risk analysis as a basis, becomes a correct authorization allocation in each individual case.

Aleris has stated that there are restrictions regarding users access options in TakeCare then the company by choosing different functions for different users can steer away users' access capabilities in the journal system.

According to Aleris, all users have different read permissions in the journal system depending on the system features they have access to. Of the document However, “Needs and risk analysis- TakeCare” states that all professional profiles in addition to technicians, read access has been assigned to the tasks in TakeCare. Furthermore, the document "Profiles and Permissions" states that all occupational profiles, ie. doctors, nurses, assistant nurses, paramedics, secretary, administrative, student and receptionist Rehab has authority to "read journal text". This means that virtually all professional profiles has access to Aleri's personal data about patients in TakeCare. The limitation that has been introduced is that different professional profiles have different ones reading privileges, for example, doctors, nurses, paramedics can read diagnoses ”or“ read prescriptions ”while other professional profiles, for example "Administratively" do not have those powers. It also appears that doctors are

the only ones who have the authority to "read emergency information".

The Data Inspectorate considers it positive that Aleris has allocated different

read permissions in the system, but that it is not enough because all

professional profiles still have access to the journal texts in TakeCare.

In addition, the division is rough as it is only a division from the outside

professional categories and not based on, for example, which organizational

affiliation, what tasks the user has or which patients

personal data that the user needs to access at different times

to. Because different users have different tasks within different

work areas, users need access to personal data about

patients in TakeCare are limited to reflect this.

Against this background, the Data Inspectorate can state that Aleris does not have

restricted users 'permissions to access patients'

personal data in the journal system TakeCare. This in turn means that one

majority of users have had actual access to the care documentation

about a large number of patients in TakeCare.

The review also shows that Aleris uses so-called active choices

for access to personal data about patients and the record filter function.

The fact that Aleris uses active choices does not mean that the access option to

personal data in the system has been restricted to the user, without the data

are still electronically accessible. This means that the active choices are not

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

as this provision requires that jurisdiction be limited to what

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

health care and that only those who need the information should have

access. The Data Inspectorate thus considers that Aleri's use of active choices

is an integrity enhancing measure but that it does not affect the actual

the access possibilities.

Aleris has further stated that there are features in TakeCare for that one

care providers must be able to "isolate" a care unit and thereby "shut out"

other care providers 'and care units' access possibilities to the unit's

care documentation, so-called protected units. However, Aleris believes that

the company does not conduct any business that requires protected entities and

have therefore not used this function.

As for the unified record keeping, all users at Aleris have

access to all personal data about patients at the other care providers in

TakeCare, except when patients have requested that their data be blocked.

It appears from the review that the care provider has an opportunity to actively

block the records of other caregivers, but that Aleris has chosen not to do so

because the company does not conduct any business that needs to be blocked. Aleris

considers it safer to leave the data at Aleri's units

available to other caregivers.

That the allocation of authorizations has not been preceded by a need and

risk analysis means that Aleris has not analyzed users' needs for

access to the data, the risks that such access may entail and

thus also not identifying which access is justified for the users
based on such an analysis. Aleris has thus not used suitable
measures, in accordance with Article 32, to restrict users' access to
patients' data in the medical record system. This in turn has meant that it
there has been a risk of unauthorized access and unauthorized distribution of
personal data partly within the framework of internal secrecy, partly within the framework
for the unified record keeping.

Aleris has further stated that the company has no technical possibilities to
make changes to TakeCare because Aleris has no control over it
the journal system. It also appears that Aleris, within the framework of it
coherent record keeping, may not implement certain restrictions
with reference to a decision from the Stockholm Region.

The basis of the Data Protection Ordinance is that the person responsible for personal data
has a responsibility to comply with the obligations set out in the Regulation in order to:
be allowed to process personal data in their activities at all. To take
appropriate technical and organizational measures to ensure an appropriate
security is such an obligation (see Articles 5, 24 and 32 of
the Data Protection Regulation). The Data Inspectorate thus considers that Aleris in
capacity as personal data controller can not waive the responsibility to
take the technical and organizational measures required by the above
articles.

In light of the above, the Swedish Data Inspectorate can state that Aleris
has processed personal data in breach of Article 5 (1) (f) and Article 32 (1) and
32.2 of the Data Protection Regulation in that Aleris has not restricted
users' permissions for accessing the TakeCare journal system to what

which is only needed for the user to be able to fulfill his

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. That means Aleris does not

have taken measures to ensure and, in accordance with Article 5 (2) (i)

the Data Protection Regulation, be able to demonstrate appropriate security for

personal data.

Documentation of access (logs)

Of the documentation of access (logs) that arose due to

The Data Inspectorate's inspection is as follows: date, time,

the identity of the user and the patient, the measures taken and

care unit. The same documentation appears when the user takes part

tasks within the framework of coherent record keeping.

The Data Inspectorate has nothing to recall in this part, because

the documentation of the access (logs) in TakeCare is in accordance

with the requirements set out in Chapter 4. 9 § HSLF-FS 2016: 40. Aleris has thus

have taken appropriate technical measures in accordance with Article 32 i

the Data Protection Regulation.

Choice of intervention

Legal regulation

If there has been a violation of the 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.

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

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

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

the circumstances of each individual case.

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 this context, it means that a great deal of responsibility rests on it

personal data controller to protect the data from unauthorized access,

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

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

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

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

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

this analysis must then be restricted to the individual executive.

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

hand that changes in the individual executive's duties

reason for it.

The Data Inspectorate's inspection has shown that Aleris has failed to take appropriate action

security measures to provide protection for the personal data in the record system

TakeCare by not complying with the requirements set out in the Patient Data Act and

The National Board of Health and Welfare's regulations regarding the implementation of needs and

risk analysis, before the allocation of authorizations in the system takes place and that not

restrict the right of access to what is needed to the individual

must be able to fulfill their duties in health care. The

means that Aleris has also failed to comply with the requirements of Article 5 (1) (f) and Article

32.1 and 32.2 of the Data Protection Regulation. Failure includes it

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

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

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

data protection ordinance Aleris Sjukvård AB to implement and document

required needs and risk analysis for the TakeCare medical record system and that

then, based on the needs and risk analysis, assign each user

individual access to personal data restricted to

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

duties in health care, in accordance with Article 5 (1) (f) and

Article 32 (1) and (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 basically concern Aleris

obligation to take appropriate security measures to provide protection to

personal data in accordance with the Data Protection Regulation.

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

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

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

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

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

notes that this is information that includes direct identification

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

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

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

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

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

responsibility to ensure patients' right to adequate protection for their

personal data.

Additional aggravating circumstances are the treatment of

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

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

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

there are almost 800,000 patients and just over 1,000 active users in

the journal system.

It is a central task for the person responsible for personal data to take measures

to ensure an appropriate level of safety in relation to the risk. At

the assessment of the appropriate level of safety, special consideration shall be given to those risks

which the treatment entails, in particular from accidental or unlawful destruction,

loss or alteration or to unauthorized disclosure of or unauthorized access to

the personal data transferred, stored or otherwise processed,

pursuant to Article 32 (2) of the Data Protection Regulation. The requirements for health and

the healthcare area, regarding current security measures, has been specified in

the Patient Data Act and in the National Board of Health and Welfare regulations. Of the preparatory work for

The Patient Data Act clearly states that requirements are placed on both strategic analysis and

that eligibility is assigned individually and adapted to the current one

the situation. That large amounts of sensitive personal data are processed without

basic regulations in the area are followed means that the procedure is assessed as

more serious.

The Data Inspectorate also takes into account that Aleris has not chosen to restrict

access within the framework of the unified record keeping. According to Aleris
it is more patient safe to leave the data at Aleri's units
available to other caregivers. This means that Aleris has given priority away
the protection of privacy within the coherent record keeping in favor of
patient safety, which is particularly serious.
The Data Inspectorate has also taken into account that Aleris has used some
integrity measures, carried out certain restrictions with regard to
the professional qualifications of the reading categories and documented access to one
correct way.
In determining the seriousness of the infringements, it can also be stated that
the infringements also cover the basic principles set out in Article 5 (i)
the Data Protection Regulation, which belongs to the categories of more serious
infringements which may give rise to a higher penalty under Article 83 (5) (i)
the Data Protection Regulation.
All these factors mean that the violations, not to implement
a needs and risk analysis and not to limit users' permissions
to only what is needed for the user to be able to fulfill theirs
tasks in health care, is not to be judged as minor
infringements without infringements that should lead to an administrative
penalty fee.
The Data Inspectorate considers that these violations are closely related to
each other. That assessment is based on the need and risk analysis
form the basis for the allocation of the authorizations. The Data Inspectorate
therefore considers that these infringements are so closely linked
that they constitute interconnected data processing within the meaning of Article 83 (3) (i)
the Data Protection Regulation. The Data Inspectorate therefore decides on a joint

penalty fee for these infringements.

According to Article 83 (3), the administrative penalty fee may not exceed

the amount of the most serious infringement in the case of one or the same

data processing or interconnected data processing.

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.

For the purposes of calculating the amount, see Article 83 (5) (i)

Data Protection Regulation that companies committing infringements such as the current ones

Sanctions of up to EUR 20 million or four may be imposed

percent of total global annual sales in the previous financial year,

depending on which value is highest.

The term company includes all companies that conduct a financial

activity, regardless of the legal status of the entity or the way in which it operates

financed. A company can therefore consist of an individual company in the sentence one

legal person, but also by several natural persons or companies. Thus

there are situations where an entire group is treated as a company and its

total annual turnover shall be used to calculate the amount of a

infringement of the Data Protection Regulation by one of its companies.

Recital 150 in the Data Protection Ordinance states, among other things

following. […] If the administrative penalty fees are imposed on a company,

an undertaking for that purpose should be considered as an undertaking within the meaning of

Articles 101 and 102 of the TFEU […]. This means that the assessment of

what constitutes a company must be based on the definitions of competition law.

The rules for group liability in EU competition law revolve around

the concept of economic unit. A parent company and a subsidiary are considered

as part of the same economic entity when the parent company exercises one

decisive influence over the subsidiary. The Data Inspectorate therefore adds

as a starting point, the turnover for Aleris Group AB as a basis for

the calculation of the size of the penalty fee.

Aleris Group AB was formed at the end of 2019. Some turnover figures for the whole

2019 is thus not available. There is therefore no information on the annual

turnover for determining the amount of the penalty fee. Aleris has

stated that the group turnover for Aleris Group AB amounted to just over 1.2

billion between 1 October 2019 and 31 December 2019.

Recalculated for an entire year, this would correspond to a turnover of approximately 4.9

billion.

The Data Inspectorate states that the actual annual sales for Aleris

Group AB this year will be significantly higher.

In the current case, the Data Inspectorate applies a precautionary principle and

therefore estimates that the company's annual turnover at least corresponds to that of

the period October - December 2019 recalculated for the full year, ie approximately 4.9

billion. The maximum penalty amount that can be determined in the current

case is EUR 20,000,000, which is just over four percent of the company's estimated

revenue.

In view of the seriousness of the infringements and that the administrative

the penalty fee must be effective, proportionate and dissuasive

the Data Inspectorate determines the administrative sanction fee for

Aleris Sjukvård AB to SEK 15,000,000 (fifteen million).

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

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

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

Katarina Tullstedt and Malin Blixt and the lawyer Linda Hamidi participated.

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

Appendix

How to pay penalty fee

Copy for information to

The Data Protection Officer

How to appeal

If you want to appeal the decision, you must write to the 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 you received the decision. 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.