Decision

Diary no

2020-12-02

DI-2019-3844

Aleris Sjukvård AB

c/o Aleris Specialist Care Sabbatsberg

Box 6401

113 82 Stockholm

Stockholm County

Supervision according to the data protection regulation and

patient data act- needs and risk analysis and

questions about access in records systems

Table of Contents

The Swedish Data Protection Authority's decision..... 2

Statement of the supervisory case..... 3

What emerged in the case..... 3

Internal confidentiality..... 5

Coherent record keeping..... 8

Documentation of the access (logs)..... 9

Aleri's opinion on the Swedish Data Protection Authority's letter..... 9

Justification of decision..... 10

Applicable rules..... 10

The Swedish Data Protection Authority's assessment..... 15

Choice of intervention..... 23

Appendix..... 29

Copy for the information of..... 29

How to appeal..... 29

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

The Swedish Data Protection Authority

DI-2019-3844

The Swedish Data Protection Authority's decision

The Swedish Data Protection Authority has, during an inspection on April 8, 2019, found that Aleris Sjukvård AB processes personal data in violation of article 5.1 f and 5.2 as well as article 32.1 and 32.2 of the data protection regulation1 by

1. Aleris Sjukvård AB has not carried out a needs and risk analysis before authorizations are assigned in the TakeCare records system, i in accordance with ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act (2008:355) and ch. 4 § 2 The National Board of Health and Welfare's regulations and general advice 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 demonstrate that the processing of the personal data has a security that is suitable in relation to the risks.

2. Aleris Sjukvård AB does not limit users' authorizations for access to the TakeCare records system to what is only needed for that the user must be able to fulfill his duties in health and medical care according to ch. 4. § 2 and ch. 6 Section 7 of the

Patient Data Act and 4

Cape. Section 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 demonstrate a suitable

security of personal data.

Datainspektionen decides with the support of articles 58.2 and 83 i

data protection regulation to Aleris Sjukvård AB, for violation of

article 5.1 f and 5.2 and article 32.1 and 32.2 of the data protection regulation,

must pay an administrative sanction fee of 15,000,000 (fifteen

million) kroner.

Datainspektionen orders with the support of article 58.2 d i

data protection regulation Aleris Sjukvård AB to implement and document

required needs and risk analysis for the TakeCare records 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 natural persons with regard to the processing of personal data and on that

free flow of such data and on the repeal of Directive 95/46/EC (general

data protection regulation).

individual authorization for access to personal data which is limited to

only what is needed for the individual to be able to fulfill their duties

tasks within the health and medical care, in accordance with article 5.1 f and

article 32.1 and 32.2 of the data protection regulation, ch. 4 § 2 and ch. 6 Section 7

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

Account of the supervisory matter

The Data Inspectorate's supervision was initiated by means of a supervisory letter on 22 March 2019 and has taken place both in writing and through an on-site inspection on April 8 2019. The supervision has intended to check 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 assigned authorizations for access to the TakeCare main record system, and which access opportunities the assigned permissions provide within the scope of as well as the internal secrecy according to ch. 4 the Patient Data Act, as the consolidated record keeping according to ch. 6 the patient data act. In addition to this have The Swedish Data Protection Authority reviewed the documentation of access (logs) which is in the journal system.

The Swedish Data Protection Authority has only reviewed the user's access to the journal system, i.e. which care documentation the user can actually take part of and read. The inspection did not cover which functions were included the authorization, i.e. what the user can actually do in the records system (eg issuing prescriptions, writing referrals, etc.).

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

What emerged in the case

Aleris has essentially stated the following.

Personal data responsibility

Aleris is a care provider and personal data controller.

The business

Aleri's ownership structure has changed after the Data Inspection Authority's review was initiated. Aleri's new ownership structure is shown in Aleri's supplement from the 16 November 2020. The addition shows, among other things, the following.

Since 1 October 2019, Aleris has been included in the newly formed group parent company, Aleris Group AB (org. no. 559210-7550), and is a subsidiary of Aleris Healthcare AB (org. no. 556598–6782). Aleris Group AB is owned by Triton.

Group turnover for Aleris Group AB amounted to SEK 1,215,385,000 between October 1, 2019 and December 31, 2019. Because Aleris Group AB was formed in connection with the change of ownership when Aleris Healthcare AB with 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

Since May 28, 2012, Aleris has been using TakeCare as the main record system for the internal secrecy and within the framework of the cohesive record keeping.

Federation Samverkan TakeCare (FSTC) is the customer of the records 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 of the records system are created by CGM, but it is Aleris that

chooses which functions a certain staff category should have access to

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

changes in TakeCare as 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. For example, the company has pointed out that there were problems

with the record system consisting in, as far as the authorization assignment is concerned, that

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

CGM has not been interested in changing this despite views from

Aleris.

It is the FSTC that can order changes to the functions and that's it

up to CGM whether 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 attention 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 these who were deceased could not be retrieved.

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

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

Internal confidentiality

Aleris has essentially stated the following.

Needs and risk analysis

Aleris has stated that needs and risk analyzes aimed at TakeCare are being carried out by an appointed risk analysis team in order to review the current authorization allocation and possibly determine new conditions for authorization allocation. 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 impropriety access is always balanced against each other before permissions are granted. General authorization profiles exist, if necessary, specific authorizations are assigned. The later reviewed in particular during subsequent analysis by appointed risk analysis team. What which are particularly taken into account are the risks that may arise if an employee has too broad authorization versus too low authorization and thus no access to relevant patient information. The result from the needs and risk analysis is then the basis for choosing the authorization profile used for assignment of authorizations within Aleris.

Entitlement to TakeCare is ordered by the responsible manager, as can be seen from the document, "Entitlement management TakeCare". It is also clear from the document that the authorization is personal and that its scope is based on

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

Aleris has a document called "Needs and risk analysis - TakeCare". The document has looked as it does today since May 28, 2012 when TakeCare was introduced and applies both to the internal secrecy and within the framework of it coherent record keeping. The document shows the different profiles, so-called authorization groups. The document shows, among other things the read and write rights for each authorization group.

All profiles except technicians have been assigned read access to the tasks in TakeCare. The eligibility of each group has been justified. The doctors are coming for example being able to perform their duties and being responsible for patient information, while the system administrator must be able to debug, administer and post users, systems and local administrators.

Under the heading "Risk of limited access" it is stated that the user "cannot perform their duties fully". This justification is stated for all profiles (except the local administrators where the justification is "Can't manage authorizations and implement corrective actions"). During the heading "Risk in case of extensive access" states, among other things, that "There is a risk of disclosure of patient information". Similar justification is given for all profiles.

Authorization assignment regarding access to personal data about patients

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

the permissions within the device. What authorization an administrator imposes

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

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

to get by" in terms of accessibility. However, access can

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

who receive the necessary authorization to be able to carry out their duties

duties. If the manager judges that the assistant nurses need one

extended permission, the local administrators ensure that the permission

"put on" 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 based on the document, "Needs and risk analysis TakeCare". As previously mentioned, it

appears from the document that all

professional profiles other than technicians have been assigned read access to the tasks i

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, access to TakeCare can be turned off

by giving different personnel authorization for different functions. Each

staff category only get access to the functions they need for

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

depending on what they will do in the system. They only get read access if they

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

will sit in the cash register and thus do not need to have a read permission.

There is no staff whose sole task is to manage 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. in terms of certifying, signing,

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

authorization to. Among these functions, Aleris has selected the functions that

different staff categories need to have access to in order to run a safe

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

authorizations that the respective staff category has been assigned in TakeCare, e.g.

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

vidimering, read referral, administer medication prescription, read scans

documents and approve care opportunities. The document shows, among other things

that all profiles, i.e. doctors, nurses, assistant nurses,

paramedic, secretary, "administrative", student and "Receptionist

Rehab" has authorization to "read journal text" and that everyone except

"Receptionist Rehab" has permission to "read scanned documents" i

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

emergency duties" and that all profiles except assistant nurse and

"administratively" 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 on the unit. One

users who need to read journal entries from another device must

make an active choice in the system. Active choices mean that the user can make a number of "clicks" and select the current device (this function is called journal filter). Permission 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 must be able to "isolate" a 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 activity that requires protected devices and therefore has not used opt out 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 assignment regarding access to personal data about patients

Authorization is assigned in the same way as within the framework of the internal the 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 healthcare providers, but not which ones. To be able to see who these caregivers are, the user must

click further in the system, i.e. make active choices. The user must then

click the “consent” or “emergency access” box to access it

specific health care provider's records.

Aleris has stated the following on the grounds that 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 it

outside the access possibilities of other care providers and care units (so-called

protected devices). A healthcare 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 carry out any activities that

need to be blocked and that it is more patient-safe to allow patient information

at Aleri's units be available to other healthcare providers. According to Aleris, it is

moreover, not allowed to implement such restrictions if one

care providers use the record system TakeCare and at the same time are included in

coherent record keeping. This is after a decision from Region Stockholm. The

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

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

have their data blocked (a so-called caregiver block).

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

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

in TakeCare (with the exception of protected devices). Either is the caregiver

included in the system for coherent record keeping or not. It is not possible to restrict access by authorized persons to other healthcare providers' information and at the same time meaningfully participate in coherent record keeping.

According to Aleris, it is not possible to determine in advance which data is in one a certain case can be important for patient-safe care. Aleris has therefore decided not to actively block other healthcare providers' records. However, can, such as mentioned, a caregiver himself blocks other caregivers' access in TakeCare there these have made the assessment that their patients' medical records should not be available to other healthcare providers. 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 the access (logs)

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

Aleris has the ability to perform targeted log checks. This means that Aleris can see exactly what a user has done in the system. About the patient or Aleris suspects a data breach, 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 choices 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 data with another healthcare provider, this will

appear from the log documentation.

Aleri's opinion on the Swedish Data Protection Authority's letter

Aleris has comments on the letter Final communication before decisions that

received by the Swedish Data Protection Authority on March 20, 2020 stating, among other things, the following.

The Swedish Data Protection Authority should take into account the figures for the economic unit where they

the alleged deficiencies took place, i.e. Aleris Sjukvård AB.

Aleris has actively worked to continuously strengthen the internal and external

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

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

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

Justification of decisions

Applicable rules

The Data Protection Regulation the primary legal source

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

is the primary legal regulation when processing personal data. This

also applies in healthcare.

The basic principles for processing personal data are stated in

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

security according to Article 5.1 f, which states that the personal data must be processed

in a way that ensures appropriate security for the personal data,

including protection against unauthorized or unauthorized processing and against loss,

destruction or damage by accident, using appropriate

technical or organizational measures.

From article 5.2 it appears that the so-called the liability, i.e. that it

"personal data controllers must be responsible for and be able to demonstrate that they

the basic principles in point 1 are complied with'.

Article 24 deals with the responsibility of the personal data controller. Of Article 24.1

it appears that the person in charge of personal data is responsible for carrying out appropriate

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

the processing is carried out in accordance with the data protection regulation. The actions shall

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

and purpose as well as the risks, of varying degree of probability and seriousness, for

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

if necessary.

Article 32 regulates security in connection with processing. According to point 1

must the personal data controller and the personal data assistant with consideration

of the latest developments, implementation costs and treatment

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

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

the personal data controller and the personal data assistant take appropriate measures

technical and organizational measures to ensure a level of security

which is appropriate in relation to the risk (…). According to point 2 shall at

the assessment of the appropriate security level special consideration is given to the risks that

the processing entails, in particular from accidental or illegal destruction,

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

the personal data transferred, stored or otherwise processed.

Recital 75 states that when assessing the risk of natural persons

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

personal data subject to confidentiality, information about health or

sexual life, if there is processing of personal data concerning vulnerable physical

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

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

Furthermore, it follows from reason 76 that how probable and serious the risk for it

Data subjects' rights and freedoms should be determined based on the processing

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

basis of an objective assessment, through which it is determined whether

the data processing involves a risk or a high risk.

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

closer to the meaning of the data protection regulation's requirements for security at

Processing of personal data.

The Data Protection Regulation and the relationship with supplementary national

regulations

According to Article 5.1. a in the data protection regulation, the personal data must

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

legal basis in that at least one of the conditions in Article 6.1 is met.

Provision of health care is one such task of generality

interest referred to in Article 6.1 e.

In healthcare, the legal bases can also be legal

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

updated.

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

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

6.2, retain or introduce more specific provisions to adapt

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

National law can further determine specific requirements for data processing

and other measures to ensure legal and fair treatment. But

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

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

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

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

special provisions to adapt the application of the provisions of

data protection regulation. Union law or Member States' national law

right must fulfill an objective of public interest and be proportionate to it

legitimate goals pursued.

Article 9 states that treatment of special categories of

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

personal data includes, among other things, information about health. Article 9.2 states

the exceptions where sensitive personal data may still be processed.

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

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

provision of healthcare on the basis of Union law or

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

health area and provided that the conditions and safeguards which

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

This means that both the legal bases public interest,
exercise of authority and legal obligation such as treatment of sensitive
personal data with the support of the exception in Article 9.2 h needs
supplementary rules.

Supplementary national regulations

For Swedish purposes, both the basis for the treatment and the
the special conditions for processing personal data within health and
healthcare regulated in the Patient Data Act (2008:355) and
the patient data regulation (2008:360). In ch. 1 Section 4 of the Patient Data Act states that
the law supplements the data protection regulation.

The purpose of the Patient Data Act is that information management within health and
healthcare must be organized so that it caters for patient safety and
good quality and promotes cost efficiency. Its purpose is also to
personal data must be designed and otherwise processed so that patients' and
the privacy of other data subjects is respected. In addition, must be documented
personal data is handled and stored so that unauthorized persons do not gain access
them (Chapter 1, Section 2 of the Patient Data Act).

The supplementary provisions in the Patient Data Act aim to
take care of both privacy protection and patient safety. The legislature has
thus, through the regulation, a balance has been made in terms of how
the information must be processed to meet both the requirements for patient safety
such as the right to personal integrity in the processing of personal data.

The National Board of Health and Welfare has issued regulations with the support of the patient data regulation and general advice on record keeping and processing of personal data i health care (HSLF-FS 2016:40). The regulations constitute such supplementary rules, which must be applied when healthcare providers treat personal data in healthcare, see ch. 1 Section 1 of the Patient Data Act.

National regulations that supplement the data protection regulation's requirements for security can be found in chapters 4 and 6. the Patient Data Act and chs. 3 and 4 HSLF-FS 2016:40.

Requirement to carry out a needs and risk analysis

The care provider must according to ch. 4. § 2 HSLF-FS 2016:40 make a need-and risk analysis, before assigning authorizations in the system takes place.

That an analysis of the needs as well as the risks is required is evident from the preparatory work to the Patient Data Act, prop. 2007/08:126 pp. 148-149, as follows.

Authorization for the staff's electronic access to information about patients must be limited to what the executive needs to be able to perform his duties in health and healthcare. It includes, among other things, that authorizations must be followed up and changed or restricted accordingly hand as changes in the individual executive's duties give rise to it.

The provision corresponds in principle to Section 8 of the Care Register Act. The purpose of the provision is to inculcate the duty of the responsible health care provider to make active and individual authorization assignments based on analyzes of which detailed information different personnel categories and different types of operations need. But it is not only necessary needs analyses. Risk analyzes must also be carried out where different types of risks are taken into account such as

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

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

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

may require special risk assessments.

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

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

categories of healthcare professionals to electronic access to records i

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

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

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

unjustified dissemination of medical records within a business and as such should

not accepted.

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

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

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

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

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

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

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

limited to single persons.

Internal confidentiality

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

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

and especially employees' opportunities to prepare for access to

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

organisation.

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

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

Coherent record keeping

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

Of ch. 6 Section 7 of the Patient Data Act follows that the regulations in ch. 4 Sections 2 and 3 also apply to authorization assignment and access control in the event of a joint operation record keeping. The requirement that the healthcare provider carry out a needs and risk analysis before the assignment of authorizations in the system takes place, thus also applies in systems

for consistent record keeping.

Documentation of access (logs)

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

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

automatically documented and systematically checked.

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

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

actions taken with data about a patient;

2. the logs show which care unit or care process

the measures have been taken,

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

4. the identity of the user and the patient can be seen in the logs.

The Swedish Data Protection Authority's assessment

Personal data controller's responsibility for security

As previously described, it is stated in article 24.1 of the data protection regulation one

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement partly aims to ensure that

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

the data protection regulation, partly that the person in charge of personal data must be able to

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

data protection regulation.

The security in connection with the treatment is regulated more specifically in the articles

5.1 f and 32 of the data protection regulation.

Article 32.1 states that the appropriate measures must be both technical and organizational and they must ensure a level of security that is appropriate in relation to the risks to the rights and freedoms of natural persons which the treatment entails. It is therefore necessary to identify the possible ones the risks to the rights and freedoms of the data subjects and assesses the likelihood of the risks occurring and the severity if they occur.

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

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

It is therefore natural that the possibilities of digitization are taken advantage of so much as possible in healthcare. Since the Patient Data Act was written, one has a lot extensive digitization has taken place in healthcare. As well as the data collections size as how many people share information with each other has increased substantially. This increase means at the same time that the demands on it increase personal data controller, because the assessment of what is an appropriate safety is affected by the extent of processing.

It is also a matter of sensitive personal data and the data concerned people who are in a dependent situation when they are in need of care.

It is also often a question of a lot of personal data about each of these persons and that the data may over time be processed by very

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

personal data controller.

The data that is processed must be protected against external actors as well

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

it is noted that in article 32.2 it is stated that the person in charge of personal data, at

assessment of the appropriate security level, in particular must take into account the risks of

accidental or unlawful destruction, loss or unauthorized disclosure or

unauthorized access. In order to know what is an unauthorized access must

the personal data controller is clear about what constitutes an authorized access.

Needs and risk analysis

In ch. 4 § 2 The National Board of Health and Welfare's regulations (HSLF-FS 2016:40), which supplement

the patient data act, it is stated that the care provider must make a needs assessment

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

national law prescribes requirements for an appropriate organizational measure that shall

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

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

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

with an excessively wide allocation of authorization for access to personal data

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

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

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

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

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

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

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

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

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

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

comprehensive an information system is, the greater the variety

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

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

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

updated.

In summary, the regulation requires that the risk analysis identifies

- different categories of data,

- categories of data subjects (for example, vulnerable natural persons and

children), or

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

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

significant social or economic disadvantage, deprivation of rights

and freedoms),

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

Processing of personal data. This also applies to internal confidentiality

as with coherent record keeping.

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

based on whether there are protected personal data that are

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

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

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

the risk to the rights and freedoms of the data subjects is based on

the nature, scope, context and purpose of the processing (reason 76).

It is thus through the needs and risk analysis that it

data controller finds out who needs access, which

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

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

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

then lead to the technical and organizational measures needed to

ensure that no other access than that which is necessary and

the risk analysis shows is justified should be able to take place.

When a needs and risk analysis is missing prior to granting authorization i

system, there is no basis for the personal data controller on a legal basis

way must be able to assign their users a correct authorization. The

personal data controller is responsible for, and must have control over, it

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

assign users a case of access to the record system, without this being established

on a performed needs and risk analysis, means that the personal data controller

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

the record system and also cannot show that he has the control that

is required.

Aleris has stated that the authorizations are assigned based on the document, "Needs and risk analysis - TakeCare". The

document shows that all

authorization profiles other than technicians have been assigned read authorization in the system,

and that the risk with limited access is that the user cannot perform their tasks

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

Furthermore, it is stated that the only risk with extensive access is that 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 Swedish Data Protection Authority can state that the document, "Needs and risk analysis TakeCare" 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 therefore not analyzed which one

information that it is a question of or how the needs look like in the different

the operational parts and for different professional roles. The document also lacks one

analysis of the risks to the individual's freedoms and rights as too broad

authorization may entail. The needs and risk analysis must take place on a strategic basis

level that should provide an authorization structure that is adapted to the business.

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

deficient in relation to the information required for a correct

needs and risk analysis must be able to be carried out. As stated above shall in a

needs and risk analysis, both the needs and the risks are assessed based on them information that needs to be processed in the business, what processes it is the question of and which risks to the individual's integrity exist both on organizational as well as individual level.

In its analysis, Aleris has not considered how negative consequences for data subjects, different categories of data, categories of data subjects or the extent of the number of personal data and data subjects affects the risk of the rights and freedoms of natural persons in Aleri's processing of personal data in TakeCare. There are also no special risk assessments based on whether there is, for example, protected personal data that is classified as confidential, information about publicly known people, information from

certain practices or medical specialties or other factors such as require special protective measures. There is also no assessment of how probable and serious risk to the rights and freedoms of the data subjects deemed to be.

In light of the above, the Swedish Data Protection Authority can state that the document "Needs and risk analysis - TakeCare" does not meet the requirements that is based on a needs and risk analysis and that Aleris has not been able to demonstrate that the company has carried out a needs and risk analysis in the sense referred to in 4 Cape. § 2 HSLF-FS 2016:40, whether within the framework of internal confidentiality according to ch. 4 the Patient Data Act or within the framework of the consolidated record keeping according to ch. 6 Section 7 of the Patient Data Act. This means that Aleris does not

has taken appropriate organizational measures in accordance with Article 5.1 f and

article 32.1 and 32.2 in order to ensure and, in accordance with article 5.2,

be able to demonstrate that the processing of the personal data has a security which is

appropriate in relation to the risks.

Authorization assignment regarding access to personal data about patients

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

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

access possibilities to personal data about patients be limited to

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

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

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

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

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

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

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

unjustified dissemination of medical records within a business and should as

such is not accepted."

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

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

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

the needs and risk analysis that the personal data controller finds out about whom

who needs access, which data the access should cover, at which

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

analyzes which risks to the individual's freedoms and rights are

the treatment can lead to. The result should then lead to the technical and organizational measures needed to ensure that no allocation of authorization provides further access possibilities than the one that needs and the risk analysis shows is justified. An important organizational action is to give instructions to those who have the authority to assign permissions on how to do this should go to and what should be taken into account so that, with the needs and risk analysis as a basis, will be a correct authorization assignment in each individual case.

Aleris has stated that there are limitations regarding the users access possibilities in TakeCare then the company by choosing different functions for different users can control the access possibilities of the users i the journal system.

According to Aleris, all users have different read permissions in the journal system depending on which system functions they have access to. Of the document "Needs and risk analysis - TakeCare" shows, however, that all professional profiles except technicians have been assigned read access to the data in TakeCare. Furthermore, it appears from the document "Profiles and Rights" that all professional profiles, i.e. doctors, nurses, assistant nurses, paramedics, secretary, administrative, student and receptionist Rehab has authorization to "read journal text". This means that pretty much 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 read permissions, for example doctors, nurses, paramedics can “read diagnoses" or "reading prescriptions" while other professional profiles, for example "administrative" does not have those permissions. It also appears that doctors are

the only ones authorized to "read emergency information".

The Swedish Data Protection Authority considers it positive that Aleris has assigned various

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, which tasks the user has or which patients

personal data that the user needs to have access to at different times

to. Because different users have different tasks within different

work areas, need users' access to personal data about

patients in TakeCare are limited to reflect this.

Against this background, the Swedish Data Protection Authority can state that Aleris does not have

limited user permissions for access to patients

personal data in the TakeCare record system. This in turn means that a

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 elections

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

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

personal data in the system has been restricted for 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. 4. Section 2 of the Patient Data Act,

as this provision requires the authority to be limited to what

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

healthcare and that only those who need the information should have it

access. The Swedish Data Protection Authority therefore 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 functions in TakeCare to a

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

other healthcare providers and healthcare 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 devices and

have therefore not used this function.

As far as the coherent record keeping is concerned, all users at Aleris have

access to all personal data about patients of the other care providers i

TakeCare, except when the patients have requested to have their data blocked.

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

block other people's care providers' records, but that Aleris chose not to do so

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

believes that it is safer for patients to leave the data at Aleri's units

available to other healthcare providers.

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

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

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

thus also not identifying which access is authorized for the users
based on such an analysis. Aleris has thus not used suitable ones
measures, in accordance with Article 32, to restrict users' access to
the patients' data in the record system. This, in turn, has meant that
there was a risk of unauthorized access and unauthorized dissemination of
personal data partly within the framework of internal confidentiality, partly within the framework
for the coherent record keeping.

Aleris has further stated that the company has no technical possibilities to
make changes to TakeCare as Aleris has no control over
the journal system. It also appears that Aleris, within the framework of the
cohesive record keeping, may not implement certain limitations
with reference to decisions from Region Stockholm.

The basis of the data protection regulation is that the person in charge of personal data
has a responsibility to comply with the obligations set out in the regulation in order to
at all be allowed to process personal data in their operations. To take
appropriate technical and organizational measures to ensure a suitable
security is such an obligation (see Articles 5, 24 and 32 i
data protection regulation). The Swedish Data Protection Authority therefore considers that Aleris i
attribute of personal data controller cannot disclaim responsibility for
take the technical and organizational measures required according to the aforementioned
articles.

In light of the above, the Swedish Data Protection Authority can state that Aleris
has processed personal data in violation of Article 5.1 f and Article 32.1 and
32.2 of the data protection regulation in that Aleris has not limited
users' authorizations for access to the TakeCare records system to what

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

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

the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40. This means that Aleris does not

has taken measures to be able to ensure and, in accordance with Article 5.2 i

data protection regulation, be able to demonstrate a suitable security for

the personal data.

Documentation of access (logs)

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

The Data Inspectorate's review shows the following: date, time,

the identity of the user and the patient, what measures have been taken and

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

data within the framework of coherent record keeping.

Datainspektionen has nothing to recall in this part, because

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

with the requirements that appear in ch. 4. Section 9 HSLF-FS 2016:40. Aleris has thus

taken appropriate technical measures in accordance with Article 32 i

data protection regulation.

Choice of intervention

Legal regulation

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

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

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

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

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

specific period.

It follows from Article 58.2 of the Data Protection Ordinance that the Data Inspectorate i

pursuant to Article 83 shall impose penalty charges in addition to or instead of

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

the circumstances of each individual case.

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

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

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

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

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

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

penalty fee.

Order

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

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

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

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

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

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

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

safety is affected by the extent of processing.

In this context, it means that a great responsibility rests on it

personal data controller to protect the data from unauthorized access,

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

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

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

there is an actual analysis of the risks based on an integrity perspective

can occur in the event of an excessive assignment of authorization to access. From

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

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

hand that changes in the individual executive's duties provide

reason for it.

The Data Inspectorate's supervision has shown that Aleris has failed to take appropriate measures

security measures to protect the personal data in the records 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 implementation of need-and

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

limit the authorization for access to what is necessary for the individual

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

means that Aleris has also failed to comply with the requirements in Article 5.1 f and Article

32.1 and 32.2 of the data protection regulation. The omission includes both

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

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

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

data protection regulation Aleris Sjukvård AB to implement and document

required needs and risk analysis for the TakeCare records system and that

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

individual authorization for access to personal data which is limited to

only what is needed for the individual to be able to fulfill their duties

tasks within the health and medical care, in accordance with article 5.1 f and

article 32.1 and 32.2 of the data protection regulation, ch. 4 § 2 and ch. 6 Section 7

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

Penalty fee

The Swedish Data Protection Authority can state that the violations basically relate to Aleris

obligation to take appropriate security measures to provide protection to

personal data according to the data protection regulation.

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

personal data and extensive permissions. The caregiver needs to

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

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

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

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

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

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

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

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

extent and the patients' dependency status give care providers a special

responsibility to ensure patients' right to adequate protection for their

personal data.

Further aggravating circumstances are that the treatment of

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

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

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

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

the journal system.

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

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

the assessment of the appropriate security level must take special account of the risks

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

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

the personal data transferred, stored or otherwise processed,

according to article 32.2 of the data protection regulation. The requirements for health and

the healthcare area, currently applicable security measures, have been specified in

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

The Patient Data Act clearly states that requirements are placed on strategic analysis as well as

that authority allocation takes place individually and is 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 Swedish Data Protection Authority also takes into account that Aleris has not chosen to restrict

the access within the framework of the coherent record keeping. According to Aleris
is it safer for patients to leave the data at Aleri's units
available to other healthcare providers. This means that Aleris has prioritized away
privacy protection within the coherent record keeping for the benefit of
patient safety, which is particularly serious.
The Swedish Data Protection Authority has also taken into account that Aleris has used certain
privacy-enhancing measures, carried out certain restrictions regarding
the professional categories' reading authorization as well as documented access on one
correct way.
When determining the seriousness of the violations, it can also be established that
the violations also include the fundamental principles of Article 5 i
the data protection regulation, which belongs to the categories of more serious
Violations that may result in a higher penalty fee according to Article 83.5 i
data protection regulation.
These factors together mean that the violations, not to implement
a needs and risk analysis and not to limit user permissions
to only what is needed for the user to be able to fulfill their
duties within the health care, are not to be assessed as minor
violations without violations that shall lead to an administrative
penalty fee.
The Swedish Data Protection Authority believes that these violations are closely related to
each other. That assessment is based on the fact that the needs and risk analysis must
form the basis for the assignment of the authorizations. The Swedish Data Protection Authority
therefore considers that these violations are so closely related to each other
that they constitute connected data processing according to Article 83.3 i
data protection regulation. The Swedish Data Protection Authority therefore determines a joint

penalty fee for these violations.

According to Article 83.3, the administrative sanction fee may not exceed

the amount of the most serious violation if it is one or the same

data processing or connected data processing.

The administrative penalty fee must be effective, proportionate and

deterrent. This means that the amount must be determined so that it

the administrative sanction fee leads to correction, that it provides a preventive measure

effect and that it is also proportionate in relation to current as well

violations as to the solvency of the subject of supervision.

As regards calculation of the amount, Article 83.5 i

data protection regulation that companies that commit violations such as those in question

may be subject to penalty fees of up to twenty million EUR or four

percentage of the total global annual turnover in the previous financial year,

depending on which value is the highest.

The term company includes all companies that conduct an economic

business, regardless of the entity's legal status or the manner in which it

be 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

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

From consideration reason 150 in the data protection regulation appears, among other things

following. […] If the administrative penalty charges are imposed on a company, should a company for this purpose be deemed to be a company 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 unity. A parent company and a subsidiary company are considered as part of the same economic entity when the parent company exercises one decisive influence over the subsidiary. The Swedish Data Protection Authority therefore puts as a starting point the turnover for Aleris Group AB as a basis for the calculation of the amount of the penalty fee.

Aleris Group AB was formed at the end of 2019. Some turnover figures for the whole 2019 is therefore not available. There is therefore no information on the annual turnover for determining the size of the penalty fee. Aleris has stated that the group turnover for Aleris Group AB amounted to just over 1.2 SEK billion between 1 October 2019 and 31 December 2019. Converted for a full year, it would correspond to a turnover of approximately 4.9 billion kroner.

The Swedish Data Protection Authority notes that the actual annual turnover for Aleris Group AB this year will be significantly higher.

In the current case, the Data Protection Authority 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 a full year, i.e. approximately 4.9

billion kroner. The highest sanction amount that can be established in current

case is EUR 20,000,000, which is roughly four percent of the company's estimate

revenue.

In light of the seriousness of the violations and that the administrative

the penalty fee must be effective, proportionate and dissuasive

the Data Inspectorate determines the administrative penalty fee for

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

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

presentation by IT security specialist Magnus Bergström. At the final

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

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

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

Appendix

How to pay penalty fee

Copy for information

The data protection officer

How to appeal

If you want to appeal the decision, you must write to the Swedish Data Protection Authority. Enter in

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

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

the day you were informed of the decision. If the appeal has been received in time

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

examination.

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.