Registered mail

Haga Hospital Foundation

[CONFIDENTIAL]

PO Box 40551

2504 LN THE HAGUE

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose an administrative fine and an order subject to periodic penalty payments

Dear [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to grant the Haga Hospital Foundation (Haga Hospital) a

to impose an administrative fine of € 460,000, because the Haga Hospital in the period from January

2018 to date has failed and failed to meet the requirement of two-factor authentication and the

regularly review log files. As a result, it has not taken adequate appropriate measures

as referred to in Article 32, first paragraph, of the General Data Protection Regulation (GDPR). the AP

has also decided to impose an order subject to periodic penalty payments on the Haga Hospital, which relates to the

undo this continuing violation.

The decision is explained in more detail below. Chapter 1 is an introduction and Chapter 2 describes it legal framework. In Chapter 3, the AP assesses its authority, the processing responsibility and the violation. In Chapter 4 the (level of the) administrative fine is elaborated and Chapter 5 shows the order subject to penalty. Chapter 6 contains the dictum and the remedies clause.

1

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Introduction

Legal entities involved

1.

1.1

The Haga Hospital is a foundation with its registered office at Els Borst-Eilersplein 275, (2545 AA) in The Hague. The Haga Hospital was founded on 1 July 2004 and is in the register of the Chamber of Commerce registered under number 27268552. In 2017 the Haga Hospital (completed) had a total of 28,500 admissions, 158,000 first outpatient clinic visits, 52,000 first aid consultations and 143,000 nursing days.1

The Reinier Haga Group Foundation (hereinafter: RHG) has its registered office at the same address as the HagaHospital. RHG was founded on July 12, 2013 and is in the register of the Chamber of Commerce registered under number 58365710. RHG is formed by Stichting Reinier de Graaf Groep, Langeland Hospital Foundation and the Haga Hospital.

1.2

Process sequence

On April 4, 2018, the Haga Hospital reported a data breach to the AP.2 The data breach had

relates to unlawful access to a patient file of a well-known Dutch person.

As a result of that notification, the AP sent a written request for information by letter dated 23 April 2018 sent to the Haga Hospital. The Haga Hospital has followed this up with a letter dated 15 May 2018 given.

In response to the information sent by the Haga Hospital, the AP has, in accordance with Article 58, first paragraph, under b, of the GDPR, decided to further investigate, insofar as this is applicable importance, access to patient data in the digital patient files at the Haga Hospital. By letter of 12 October 2018, the AP sent a written request for information to the HagaHospital. Haga Hospital has complied with this.

On October 31, 2018, an announced on-site investigation (hereinafter: OTP) at the Haga Hospital occurred.

By letter dated November 19, 2018, the AP denied the business representation of the relevant statements of the employees of the Haga Hospital sent to the Haga Hospital during the OTP with the possibility to make known the factual (in)correctness of the statements.

By letter dated 29 November 2018, Haga Hospital submitted its comments on the aforementioned reports made known.

1 In this context, the AP refers to the figures from the Annual Report submitted by the Haga Hospital for its opinion hearing.

2 Report number [CONFIDENTIAL].

The record of the conversations that took place during the OTP is - taking into account the response of the Haga Hospital on the business representation of the statements - on December 19, 2018 by the AP established.

The results of the further investigation are recorded in the report “Access to digital patient records by employees of the Haga Hospital, Preliminary findings” of January 2019 (hereinafter: report preliminary findings).

Given the opportunity to do so by the AP on 16 January 2019, the Haga Hospital has informed letter of February 4, 2019 has given its response to the Preliminary Findings report.

Taking into account this response, the AP has adopted the final report. This report is by letter sent to the Haga Hospital on 26 March 2019.

In a letter dated April 4, 2019, the AP sent Haga Hospital an intention to impose of an administrative fine and/or an order subject to a penalty for violation of Article 32 of the GDPR.

Also given the opportunity to do so by letter of 4 April 2019 by the AP, the Haga Hospital has informed letter of April 18, 2019 has given its opinion in writing on this intention and the basis of the final report.

Reason for research

On April 25, 2019, an opinion session was held at the offices of the AP in which the HagaZiekenhuis has also verbally explained its view.

By e-mail of April 30, 2019, the Haga Hospital sent two documents upon request.

In a letter dated 16 May 2019, the AP sent the report of the opinion session to HagaZiekenhuis.

The Haga Hospital has indicated that it has no comments on the report.

1.3

On April 4, 2018, the Haga Hospital reported a data breach to the AP. The data breach had relates to unlawful access to a patient file of a well-known Dutch person. In the notification Haga Hospital announces that pending the internal investigation into unlawful access of this patient file will take security measures.

The results of this internal investigation are included in the report “Final Report Investigation unlawful access to patient file” of May 2018. This report states that the Haga Hospital structural random checks whether authorized employees are within the applicable frameworks

consult patient records. If in doubt, an investigation will follow. Similarly, an investigation into the

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Scope GDPR

(possibly) unlawful access to the patient file concerned by the data breach, according to the report.3 In

the report states that in the period examined 197 employees, of which 100 illegally,4 access

have in the patient record. The Haga Hospital concludes that the solution must

lead to a structural improvement, for which the present and future measures

must be regularly tested for correct operation and, if necessary, must be

adjusted.5

As a result of the aforementioned report, the AP decided in October 2018, among other things, to investigate further

to the security measures of the Haga Hospital.

2. Legal framework

2.1

Pursuant to Article 2(1) of the GDPR, this Regulation applies to all or part of

automated processing, as well as to the processing of personal data that are in a file

included or intended to be included therein.

Pursuant to Article 3(1), this Regulation applies to the processing of personal data

in the context of the activities of an establishment of a controller or a processor

in the Union, whether or not the processing takes place in the Union.

Pursuant to Article 4, for the purposes of this Regulation:

1. “Personal data”: any information about an identified or identifiable natural person

(“the data subject”); […].

2. “Processing”: an operation or set of operations relating to personal data or

a set of personal data, whether or not carried out by automated processes […].

7. “Controller” means a […] legal entity that, alone or jointly with others, fulfills the purpose of

and determine the means of processing personal data; […].

15. “Health data” means personal data related to the physical or mental

health of a natural person, including data on health services provided

providing information about his health status.

2.2

2.2.1 GDPR

Pursuant to Article 32(1) of the GDPR, the controller shall take into account […]

the state of the art, the implementation costs, as well as the nature, scope, context and

processing purposes and the risks of varying likelihood and severity to the rights and

3 pg. 3 of the report.

4 In its response of 4 February 2019, the Haga Hospital states that this should be 85.

5 pg. 7 of the report.

freedoms of persons, appropriate technical and organizational measures to

ensure an appropriate level of security […].

Pursuant to the second paragraph, in the assessment of the appropriate security level, particular account shall be taken of:

account of the processing risks, in particular as a result of the destruction, loss, alteration or

unauthorized disclosure or access to transmitted, stored or otherwise

processed data, either accidentally or unlawfully.

2.2.2 Additional Provisions for the Processing of Personal Data in Healthcare Act

Pursuant to Article 1, preamble and under m, of the Additional Provisions for the Processing of Personal Data Act in healthcare, in this Act and the provisions based on it, the following definitions apply:

“Healthcare Information System”: a healthcare provider's electronic system for processing personal data in a file, not being an electronic exchange system.

Pursuant to Article 15j, first paragraph, rules may be laid down by order in council regarding the functional, technical and organizational measures for the management, security and use of a healthcare information system or an electronic exchange system.

2.2.3 Decree on electronic data processing by healthcare providers

The Decree on electronic data processing by healthcare providers is a general measure of board as referred to in Article 15j, paragraph 1, of the Additional Provisions Processing Act personal data in healthcare.

Pursuant to Article 1, the Decree on electronic data processing by healthcare providers means: below:

“NEN 7510”: standard for the organizational and technical organization of information security in healthcare;

“NEN 7513”: further implementation of NEN 7510 regarding the recording of actions in electronic form patient records.

“Healthcare Information System”: a healthcare provider's electronic system for processing personal data in a file as referred to in the Additional Provisions Processing Act personal data in healthcare, not being an electronic exchange system.

Pursuant to Article 3, second paragraph, a healthcare provider in accordance with the provisions of NEN 7510 […] ensure safe and careful use of the healthcare information system […].

Pursuant to Article 5, first paragraph, the healthcare provider, as the person responsible for a healthcare information system […] ensure that the logging of the system complies with the provisions of NEN 7513.

2.2.4 NEN 7510 and NEN 7513

NEN 7510 of December 2017 pertains to medical informatics and information security in healthcare and exists in two parts: part 1 (7510-1) contains normative requirements for the management system and part 2 (7510-2) contains the control measures. NEN 7513 includes logging. NEN 7510 and 7513 state

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

central to the fact that information in healthcare is often confidential in nature. As a healthcare organization, therefore, measures are taken to keep patient data safe.

Two-factor authentication

In Chapter 9 (Access Security), Section 9.4 (System and Application Access Security), under 9.4.1 (Restricted access to information) of NEN 7510-2 it is stated that health information systems processing personal health information should identify users.

This should be done through authentication involving at least two factors become.

(Check on) logging

Chapter 5 (Information needs), paragraph 5.1 (General) of NEN 7513 states that the logging in the in general should make it possible to establish irrefutably afterwards which events occurred on a patient record. To this end, all systems containing data that be part of a patient file, keep at least:

- which event took place;
- date and time of the event;
- which client was involved;
- who the user was;

- who was the responsible user on whose behalf the user was acting.

In chapter 12 (Security of business operations), paragraph 12.4 (Reporting and monitoring), under 12.4.1

(Registering events) of NEN 7510-2 states that log files of events that

record user activities, exceptions and information security events should be

be created, stored and regularly reviewed.

2.3

Pursuant to Article 58, second paragraph, preamble and under d and i, in conjunction with Article 83, fourth paragraph,

preamble and

under a of the GDPR and Article 14, paragraph 3, of the UAVG, the AP is, among other things, authorized to:

to impose an administrative fine and an order subject to a penalty for infringements of the GDPR.

2.3.1 GDPR

Pursuant to Article 58, paragraph 2, of the GDPR, each supervisory authority has the power to

taking the following corrective actions:

d. order the controller […], where appropriate, in a specified manner and within

a specified period, to bring processing operations in accordance with the provisions of this

regulation;

i. as the circumstances of each case, in addition to or in lieu of the measures referred to in this paragraph,

impose an administrative fine under Article 83.

Administrative fine and order subject to periodic penalty payments

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Rating

Pursuant to Article 83(1), each supervisory authority shall ensure that the administrative

fines imposed under this Article for the infringements referred to in paragraphs 4, 5 and 6

to this Regulation are effective, proportionate and dissuasive in every case.

Under paragraph 2, administrative fines shall be, according to the circumstances of the

specific case, imposed in addition to or instead of the provisions of Article 58, second paragraph, under a to h and under j,

measures referred to.

It follows from the fourth paragraph, opening words and under a, that an infringement of the obligation of the

controller of Article 32 in accordance with paragraph 2 is subject to a

administrative fine up to € 10,000,000 or, for a company, up to 2% of the total worldwide

annual turnover in the previous financial year, if this figure is higher.

2.3.2 General Data Protection Regulation (UAVG) Implementing Act

Pursuant to Article 14, paragraph 3, of the UAVG, the AP may, in the event of a violation of the provisions of Article

83, fourth paragraph […], of the Regulation impose an administrative fine not exceeding the amount specified in these

paragraphs

mentioned amounts.

3.

Section 3.1 first assesses the authority of the AP. Subsequently, in paragraph 3.2

explains who can be regarded as a controller for which processing. The

violation of Article 32, first paragraph, of the GDPR, read in conjunction with Article 3, second paragraph, of the

Decree on electronic data processing by healthcare providers and the provisions under 9.4.1 and under 12.4.1

of NEN 7510-2, is established in section 3.3.

3.1

The Haga Hospital has a hospital information system as referred to in Article 1 of the Act

additional provisions for the processing of personal data in healthcare and Article 1 of the Electronic Decree

data processing by healthcare providers. In this system, also called the Electronic

Patient file (EPD) or HiX, data relating to patients are collected by the Haga Hospital

Hospitalized. Therefore, there is processing of personal data, including personal data

on health, as referred to in Article 4 of the GDPR.

At the time of the aforementioned data breach and the notification by the Haga Hospital to the AP on April 4, 2018,

the Personal Data Protection Act (Wbp). The Wbp was withdrawn on 25 May 2018.6 On that day, the

GDPR became applicable7 and the UAVG came into effect.8

As a result of the aforementioned data breach and the report drawn up for that purpose by the Haga Hospital

“Final report Investigation into illegal access to patient file” of May 2018, the AP has

Authority AP

6 Article 51 of the UAVG.

7 Article 99(2) of the GDPR.

8 Royal Decree of 16 May 2018 (Official Gazette 2018, 145).

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

2018 - well after the date on which the GDPR became applicable - launched a further investigation into

the security measures taken by the Haga Hospital at that time in order to ensure

that personal data in the digital patient file are not viewed by unauthorized persons

Staff members. The investigation focused, among other things, on the question of whether the

Haga Hospital has taken security measures with regard to access to the

hospital information system comply with - the then current - Article 32 of the GDPR. the AP

with regard to the violation established in the final report on the basis of Article 58, second paragraph,

preamble and under d and i, in conjunction with Article 83, fourth paragraph, preamble and under a, of the GDPR and Article

14, third paragraph, of the UAVG is authorized to impose an administrative fine and an order subject to a penalty,

if circumstances so require.

3.2 Controller

The Haga Hospital has been part of RHG since 12 July 2013. RHG is a partnership between the Haga Hospital, Reinier de Graaf Groep (both as of 12 July 2013) and the Langeland Hospital (per June 9, 2015). In the context of the question whether Article 32(1) of the GDPR is complied with, it is important to determine who is or can be designated as (joint) controller(s) as referred to in Article 4(7) of the GDPR. The determining factor here is who has the purpose and means of the processing of personal data - in this case the processing of patient data in the hospital information system of the Haga Hospital - establishes. To answer this question, the AP value to the provisions in the report “Information security policy Reinier Haga Groep” of December 25, 2015 (Information Security Policy), the Digital Patient Records Authorization report of May 2018 (Authorization Policy), the Privacy Statement of the Haga Hospital9 and the statement of [CONFIDENTIAL] as included in Report of conversations OTP Haga Hospital.

3.2.1

As was also confirmed by the Haga Hospital at the opinion session, the general part of the RHG established Information Security Policy applicable to all data processing operations in all business addresses of RHG, including the Haga Hospital.10 When applying information security within RHG, the standards NEN 7510 and NEN 7513 are used as a starting point 11 These standards are not discussed further in the general part of the Information Security Policy worked out. The Board of Directors of RHG is administratively responsible for the implementation of the information security policy and measures.12

The local implementation of the general part - which may differ per organization within RHG - is included in the appendices to the Information Security Policy. Appendix 2 concerns the local implementation by the HagaHospital. The Haga Hospital has its own Information Security Officer (ISO), who monitors Information Security Policy

9 https://www.hagaziekenhuis.nl/about-hagaziekenhuis/goed-om-te-weten/patients' rights/privacy statement.aspx.

10 pg. 4 Information Security Policy. In addition to this, the Haga Hospital has confirmed on request that the general part of this policy also applies to the Langeland Hospital Foundation.

11 pg. 9 Information Security Policy.

12 pg. 6 Information Security Policy.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

is the point of contact for all information security matters within that hospital and the local coordination of information security activities.13 All parts of RHG must have taken adequate measures to ensure the continuity of the operational activities secure. Managing - among other things - an emergency button procedure is part of this.14 The standards NEN 7510 and NEN 7513 are no longer included in Appendix 2 (Local implementation of Haga Hospital) worked out.

3.2.2 Authorization Policy

The Authorization Policy has been drawn up by Haga Hospital and contains policy for the design and systems in connection with authorization for access to the EPD within the Haga Hospital, as well as the control.15 This policy states that in hospitals, the purpose and means of processing personal data is determined by the management of the Haga Hospital.16 The management takes appropriate technical and organizational measures to protect personal data against loss or against any form of unlawful processing.17

3.2.3 Privacy statement

The Haga Hospital's Privacy Statement states that it applies to the processing of personal data by the Haga Hospital. At the hearing, the Haga Hospital explained that the RHG Privacy Regulation of 15 June 2017 serves as the basis for the Privacy Statement. The AP notes that the Privacy Regulations only contain general provisions relating to the processing of personal data. The Privacy Statement contains a further interpretation of the Privacy Regulations, on the basis of:

of which data processing by the Haga Hospital for - among others - the following therein

included purposes may be processed:

- providing, calculating the costs and claiming care;

- conducting scientific research;

- the training and education of healthcare personnel;

- administration and internal management activities;

- quality assurance and promotion of care provision.

The Privacy Statement also states that Haga Hospital also collaborates with other parties

healthcare institutions. The Haga Hospital asks the patient's permission before taking the relevant

exchange data, unless the interests of the patient or a third party are at risk.

3.2.4 Declaration Haga Hospital

On October 31, 2018, [CONFIDENTIAL] of the Haga Hospital stated during the OTP that RHG

an administrative merger and not a legal merger. For example, the hospitals are system technical

separated, the elaboration of the Authorization Policy is different per hospital and is generally

Information security policy completed locally per hospital. Each hospital also has its own

13 pg. 6 of the Information Security Policy.

14 pg. 11 of the Information Security Policy.

15 pg. 3 Authorization Policy.

16 pg. 2 Authorization Policy.

17 pg. 3 Authorization Policy.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Authorization Committee.18

3.2.5 Assessment of AP

The AP is of the opinion that the Haga Hospital aims and means of data processing in the hospital information system of the Haga Hospital - which is separate from the hospital information systems of the other hospitals of RHG - determines. In this way she determines independently the local implementation of the general Information Security Policy and has its own Authorization Policy, on the basis of which it determines who may have authorized access to which patient data. Also Haga Hospital has its own Privacy Statement, in which it explains the purposes of data processing determined by the Haga Hospital.

For the question whether the Haga Hospital alone or together with RHG makes decisions regarding the determination of purposes and means of data processing in the hospital information system of Haga Hospital, it is important that RHG only has a general Information Security Policy and a general Privacy Regulations. This established general policy does not cover a detailed level on how the hospitals within RHG set up the hospital information system. It Information security policy only ensures that the standards NEN 7510 and NEN 7513 are observed should be taken. This also follows from Article 32(1) of the GDPR, read in conjunction with Article 3, second paragraph, and Article 5, second paragraph, of the Decree on electronic data processing by healthcare providers. Furthermore, the Privacy Regulations only contain a repetition of the standards from the Wbp applicable at the time, without specifying these standards in concrete terms. Furthermore it falls partnership outside the scope of the Authorization Policy - which concerns the authorization for access to the EPD of the Haga Hospital - and the Privacy Statement of the Haga Hospital, in which among other things, the purposes of data processing for the Haga Hospital are included.

Partly in view of the statement by [CONFIDENTIAL] of the Haga Hospital, the AP has taken into account of the foregoing is of the opinion that the Haga Hospital independently has the formal legal competence has to identify the purposes and means of data processing in the hospital information system of the Haga Hospital to be established.

3.2.6 Conclusion

Now that, in the opinion of the AP ., the Haga Hospital has moved with regard to the hospital information system

autonomously, the Haga Hospital - and not also RHG - will be

data processing operations in that hospital information system as controller as referred to

referred to in Article 4, preamble and under 7, of the GDPR.

3.3 Data Security Violation

3.3.1

To ensure security and prevent the processing of personal data from infringing

Introduction

18 pg. 2 of the Report of conversations OTP Haga Hospital.

to the GDPR, the controller must, pursuant to Article 32 of the GDPR,

processing inherent risks and take measures to mitigate risks. That

measures should ensure an appropriate level of security, taking into account the status

of the technology and the implementation costs compared to the risks and the nature of the

personal data.19 Because of its sensitivity, health data belongs to a special category

of personal data. For this reason, very high requirements apply to the protection of that data.

Appropriate security measures help to maintain patient trust

in the relevant hospital when handling personal data. In order to determine whether

security measures are appropriate, should in the present case be linked to the general

accepted security standards within the practice of information security in healthcare, NEN-

7510 and NEN 7513. It follows from these security standards that with regard to authentication at the

access to hospital information systems specifically aimed at processing sensitive

information, the controller must at least use two-factor authentication, in order to establish the identity of users. In addition, log files of events that record user activities, exceptions and information security events created, stored and regularly reviewed. The foregoing follows from NEN 7510 -2, in which security standards have been included that relate to a further interpretation of Article 32 of the GDPR which means concerns information security in healthcare, according to the Authorization Policy of the Haga Hospital also refers.

3.3.2 Two-factor authentication

Section 9.4.1 of NEN 7510-2 states that health information systems containing personal processing health information, should establish the identity of users. This should be are done through authentication involving at least two factors. This means that the user's identity to access the health information system for example, it is determined on the basis of knowledge (code or a password) and possession (staff card).

Staff pass and User manual Virtual Workplace scheme

The Haga Hospital's Personnel Card Regulation20 states that all employees of the Haga Hospital have a staff card, which can be used to log in to the computers. The powers of this own identity card are related to the position and workplace of the collaborator. This pass can prevent other users from sharing confidential documents can see. You can also log in without a card, but using your username and password password. The pass is for convenience only, according to the Regulation.

The Virtual Workplace User Manual21 confirms that the workstations with a card reader suitable for virtual work. Employees can manually, but after registration also with the

19 Recital 83 of the GDPR.

20 Revision date June 13, 2017.

21 From August 14, 2018.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

register staff pass.22

Declaration Haga Hospital

During the OTP on October 31, 2018, the Haga Hospital confirmed that there are two ways:
are logged in to the computers and the hospital information system. One of the options is with
using the staff card, which is held in front of the card reader, after which you can log in
on the Virtual Desktop Infrastructure (VDI) with username, password and a 4 digit fixed
pin. A personal HiX account is attached to this personal network account. This means that if a
employee is logged in to the VDI, this employee also has access to the
hospital information system. After that, the user can spend four hours - the so-called 'grace'
period'- on any workstation with the card log out and log in without entering user name,
password and/or PIN. The other option is without using the staff card,
where you can manually log in to the VDI with username and password. Once
logged in, the employee - just like when logging in with the card - also has access to the
hospital information system.23

View

The Haga Hospital's view states that in the current situation access to the
hospital information system can be obtained through both two-factor and one-factor authentication.
During the opinion session it was explained that the Haga Hospital started with the virtual
workstations, also with the option to log in manually. It has set itself the goal of
October 1, 2019 to have implemented permanent two-factor authentication hospital-wide, whereby
the ability to log in via one-factor authentication disappears. Furthermore, the Haga Hospital will
abolish the so-called 'grace period', so that when accessing via two-factor authentication, every

PIN will be requested.

Rating API

Now that the strength of user authentication should be appropriate for the classification of the information to which access is granted, and in the hospital information system (in particular) data about health, two-factor authentication is required. The AP determines - nor does it dispute is - that authentication in the Haga Hospital to the hospital information system in any case has taken place since January 2018 and continues to take place using the unique staff pass. In the other situation, logging in without a staff card, authentication takes place based on of a username and password, after which the hospital information system can be consulted become. The identity of the user to access this system can in this case thus take place solely on the basis of knowledge (code or a password), without possession (staff card). Therefore, a single method for consulting the hospital information system by the users and lacks a necessary second factor that contributes to a appropriate security level. This does not meet the requirement of two-factor authentication

22 pg. 2 User Manual Virtual Workplace.

23 pg. 7 Statement of conversations OTP Haga Hospital and also confirmed at the opinion session.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

pursuant to Article 32 of the GDPR, read in conjunction with Article 3(2) of the Electronic Decree data processing by healthcare providers and the provisions under 9.4.1 of NEN 7510-2.

3.3.3 Regular review of log files

Healthcare institutions must keep track of who consulted which patient file and when (logging) and this should be checked regularly. In this way, the institution can prevent unauthorized

signal access and take measures. This is based on section 12.4.1 of NEN 7510-2, in which
states that event logs that record user activity, exceptions, and
record information security events, should be created, stored and regularly monitored
be assessed.
With reference to the report “Access to digital patient records within healthcare institutions” by
June 2013 the basic principle of the AP24 is that checking the logging must be systematic and consistent
take place, whereby a random check and/or check on the basis of complaints is not sufficient
is. It is important here that in a random random check there is no question of a
systematically aimed at illegal use and risks.
Authorization Policy
The Haga Hospital's Authorization Policy states that security and logging in accordance with the
starting points as stated in NEN 7510 and NEN 7513 must take place. In the
Authorization policy is based on the principle that the log files are periodically checked for
indications of unlawful access or use of personal data and action where necessary
is undertaken by the responsible person. The Authorization Policy makes a distinction in the control
of (1) regular patient files, (2) patient files belonging to specialisms and (3)
patient records that have been accessed via the so-called emergency button procedure, also known as
referred to as “breaking the glass” procedure, described in more detail below.25
Pursuant to the Authorization Policy for (1) regular patient files, the DPO must
months to perform an audit on access to the system in accordance with the established authorization procedure.
At the opinion session, the Haga Hospital explained that this should include a
check of one patient file every two months. The Haga Hospital has further explained that (2)
if a selected file belongs to treatment in the specialties of psychiatry, psychology, VIP,
own staff and in relation to venereal diseases, the logging of that file must be complete
checked. This means that the logging of this file is checked for a longer period.
Employees of the Haga Hospital can also use (3) an emergency button procedure,

with which they gain access to patient data, for which this employee is not authorized

is. The procedure does not allow searching for such patient data and actually wanting to look into it

of this data will see a notification on the screen, in which employees are informed that they are not

authorized to access this specific patient data. To the employees

24 Although under the operation of the Wbp, the purport of Article 32 of the GDPR is different from Article 13 of the

applicable Wbp not changed.

25 pg. 3 of the Authorization Policy.

asked to give a reason why access is still necessary. Using that procedure

employees can then still gain wider access to patient data. In the

Authorization policy states that a failed access attempt as well as realized access to a digital

file of a patient, which are realized via the emergency button procedure, regularly serve via the logging

to be checked for legality.

Declaration Haga Hospital

[CONFIDENTIAL] has stated during the OTP that every action is logged in the EPD. The

checks on the logging are performed by the ISO and the FG. The first inspection in 2018 concerned

patient file of the well-known Dutchman, given the large amount of insight into this specific

file.26 At the request of patients and employees, the Haga Hospital will carry out even more checks in 2018

carried out, which did not reveal any wrongdoing. [CONFIDENTIAL] further stated

that the Haga Hospital intends to carry out six random random checks per year in 2019

of the logging in accordance with the Authorization Policy, involving six different patients from

different departments will be checked. Due to the crowds due to the aforementioned data breach

and the subsequent actions, the Haga Hospital at the time of the statement of October 31, 2018 was (still)
not got around to this.

View

The Haga Hospital aims to comply with paragraph 12.4.1 of NEN 7510-2 in the
form of checking logging in the following three ways: (1) on the basis of samples
covering six patient records per year, (2) based on patient complaints and requests and (3)
through a systematic analysis of the use of the emergency button procedure. The sample (1)
is limited to six files per year because carrying out such a check is a very
is a labour-intensive process, according to the Haga Hospital. After generating the logging must be done manually
it is determined per logging line whether the person who logs in is part of the treatment team of the
concerning patient. At the opinion hearing, the Haga Hospital has, upon request, made a rough estimate
based on the scope of the audit trail, which consists of five steps. The first three steps can
are performed by one employee and monitor the generation of the logging, the completion and
monitoring and determining the treatment team. In the last two steps, further research
place, performed by several employees. The implementation of the first three steps take a total of -
and on average - about eight hours, which is about one-third to one-half of a full audit trail
according to the Haga Hospital. With regard to the control of logging, it further states that (2)
patients can also invoke the right to inspect the logging and so can the Haga Hospital in those cases
check for logging. The systematic analysis (3) includes a weekly check of the logging
of all patient records accessed via the emergency button procedure. The drafted by her
planning aimed at 1 October 2019 is based on a manual check. The possibilities of using
[CONFIDENTIAL] - as a technical aid when performing the logging check - be
still examined by the Haga Hospital.

At the opinion hearing, the Haga Hospital confirmed that in the period from January 2018 to

26 See also the response of the Haga Hospital of 4 February 2019.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

October 2018 proactive one check on logging related to the file of the well-known Dutchman

and six logging checks related to six records on patient and staff requests

has performed. After October 2018, various checks were carried out at the request of patients and/or

employees took place. The Haga Hospital started the first sample in January 2019

of the intended six samples per year. The second study is scheduled for April/May 2019 on the

planning, according to the Haga Hospital.

Rating API

The AP notes that in 2018 the Haga Hospital - with the exception of one proactive sample -

exclusively in response to a few complaints and requests. The done in 2019

proactive monitoring (covering up to two patient records) does not include a separate

control of the logging of patient records accessed via the emergency button procedure. It

HagaZiekenhuis thus has at least during the aforementioned period (January 2018 to present)

not acted in accordance with its own Authorization Policy. Apart from that, doing just one or

a few proactive sample/samples per year amply and evidently insufficient to be able to

speak of an appropriate security level that refers to signaling unauthorized access to

patient data and taking measures in response to unauthorized access. In doing so, the

AP of importance the scale of the hospital's processing of health data27 and the

lack of regular check on use of the emergency button procedure, resulting in

employees can gain access to more data than they are authorized to do in the first instance

to be. In view of this, there are no appropriate measures with regard to monitoring the logging such as

required under Article 32(1) of the GDPR, read in conjunction with Article 3(2),

Decree on electronic data processing by healthcare providers and the provisions under 12.4.1 of NEN

7510-2.

In addition, in the context of the order subject to a penalty to be imposed, the AP also answers the question of whether the Authorization policy provides for systematic, consistent control of logging data. The

The AP determines, partly on the basis of the explanation from the Haga Hospital, that the Authorization Policy provides a check on the logging of six (regular or non-regular) patient files and a regular control of patient records that have been accessed using the emergency button procedure. What should be understood by regular control of the latter files, is not further elaborated in the Authorization Policy. In the view of the Haga Hospital of April 18, 2019 it states that it aims to submit all patient files on a weekly basis by October 1, 2019 at the latest investigations consulted via the emergency button procedure. The Haga Hospital presents itself with the implementation of the intended measures, in addition to the reactive control following a complaint or request, on the view that the log files are regularly checked as intended in the NEN 7510-2. In the opinion of the AP, such a weekly check certainly meets the requirements the requirement of systematic, consistent control of logging data. However, this leaves without prejudice to the fact that Haga Hospital also increases the risk of misuse within the authorization profile with regard to

27 In this context, the AP refers to the figures from the Annual Report submitted by the Haga Hospital for its opinion hearing. In 2017

Haga Hospital (completed) 28,500 admissions, 158,000 first outpatient clinic visits, 52,000 first aid consultations and 143,000 nursing days.

of the other files - not consulted via the emergency button procedure - should be sufficiently control. Log files can be used to find out who had access to which

health data. Out of a size of - in 2017 - (rounded up) 28,500 shots, 158,000 first outpatient clinic visits, 52,000 first aid consultations and 143,000 nursing days, provides a control of six patient files annually insufficient effort to deal with cases of unlawful processing take place within the authorization to a sufficient degree to be able to detect. In the opinion of the AP this does not lead to the required appropriate level of security in cases where the file is within the authorization has been consulted.

The current state of the art is normative for what is considered appropriate measures within the meaning of Article 32(1) of the GDPR can be considered. The Haga Hospital has not plausibly made that - possibly in addition to [CONFIDENTIAL] - no other technical support options are available. The steps taken by the Haga Hospital to come to an update in that context are therefore recommended. Insofar as the Haga Hospital has no or limited has technical support to perform or support the control of logging as it has argued in the opinion, it must organize the control of the logging in an organizational manner. It To this end, Haga Hospital has proposed the logging of all files that have been consulted via the emergency button procedure manually. In view of this, it is not apparent that a manual control of the logging of more than six files - not consulted via the emergency button procedure - per years, cannot be expected of her. That the Haga Hospital, as it has at the opinion session explained, also takes preventive measures with a view to preventing unauthorized access to patient data, which include awareness among employees about careful handling with patient data, the obligation to take the aforementioned appropriate technical and organizational measures within the meaning of Article 32(1) of the GDPR.

Taking into account that the Authorization Policy covers, among other things, a check of one sample of one file every two months, in the opinion of the AP, that policy does not provide for a systematic, consistent control of the logging.

3.3.4 Conclusion

In view of the foregoing, the AP is of the opinion that the Haga Hospital has Article 32, first paragraph, of the GDPR,

read in conjunction with Article 3, second paragraph, of the Electronic Data Processing Decree by

healthcare providers and the provisions under 9.4.1 and under 12.4.1 of NEN 7510-2, now in the

period from January 2018 to date, the requirement of two-factor authentication has not been met and the

regularly review log files. The violation is now continuing.

4.

4.1

The security measures taken by the Haga Hospital do not refer to a (correct) implementation

from using two-factor authentication and checking the log files regularly. From the

Introduction

fine

16/25

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Fines Policy Rules of the Dutch Data Protection Authority 2019 (Fines Policy Rules 2019)

Haga Hospital may, however, be expected to ascertain the standards that apply to it.

Failure to use two-factor authentication in case of access to patient data - in which

paragraph 9.4.1 of NEN 7510-2 leaves no room - and only proactively check it in practice

of the logging of one or more patient file(s) over a period of more than one year, is to

the opinion of the AP - and contrary to what Haga Hospital argues - evidently and structurally in

contrary to Article 32, first paragraph, of the GDPR, read in conjunction with the provisions under 9.4.1 and under

12.4.1 of NEN 7510-2. That the Haga Hospital argued at the opinion hearing that the standard in

12.4.1 of NEN 7510-2 contains an open standard, does not change that - whatever that may be - now that the

Haga Hospital has also deviated from its own Authorization Policy in practice. This while it

According to her, the authorization policy, with the explanation it provides in the opinion, meets the standard in

12.4.1 of NEN 7510-2. In the present case, the AP sees reason to make use of its
authority to impose a fine pursuant to Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in conjunction with Article 14, third paragraph, of the UAVG, to the Haga Hospital lay.

4.2

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in In conjunction with Article 14, third paragraph, of the UAVG, the AP is authorized to appoint the Haga Hospital in the event of to impose an administrative fine of up to € 10,000,000 for a violation of Article 32, first paragraph, of the GDPR or up to 2% of the total worldwide annual turnover in the previous financial year, whichever is higher.

The AP has established Fine Policy Rules 2019 regarding the interpretation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.28

Pursuant to Article 2, under 2.1, of the Fine Policy Rules 2019, the provisions with regard to violation of which the AP can impose an administrative fine not exceeding the amount of € 10,000,000 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure higher, classified in Appendix 1 as Category I, Category II or Category III.

In Annex I, Article 32 of the GDPR is classified in category II.

Pursuant to Article 2, under 2.3, the AP sets the basic fine for violations for which a statutory maximum fine of € 10,000,000 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher, […] fixed within the next fine bandwidth:

Category II: Fine range between €120,000 and €500,000 and a basic fine of €310,000. […].

Pursuant to Article 6, the AP determines the amount of the fine by increasing the amount of the basic fine (up to at most the maximum of the bandwidth of the fine category linked to a violation) or down (to at least the minimum of that bandwidth). The basic fine will be

28 Stct. 2019, 14586, March 14, 2019.

increased or decreased depending on the extent to which the factors referred to in Article 7 to that end

give rise to.

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act

(Awb) taking into account the factors derived from Article 83, second paragraph, of the GDPR, in the

Policy rules mentioned under a to k:

the nature, seriousness and duration of the infringement, taking into account the nature, scope or purpose of the infringement

processing in question as well as the number of data subjects affected and the extent of the damage suffered by them

injury;

b. the intentional or negligent nature of the infringement;

c. the measures taken by the controller […] to address the data subjects suffered

limit damage;

d. the extent to which the controller […] is responsible given the technical and

organizational measures that he has carried out in accordance with Articles 25 and 32 of the GDPR;

e. previous relevant breaches by the controller […];

f. the extent to which there has been cooperation with the supervisory authority to remedy the breach and

limit the possible negative consequences thereof;

g. the categories of personal data to which the breach relates;

h. the manner in which the supervisory authority became aware of the infringement, in particular whether, and

if so, to what extent, the controller […] has notified the breach;

i. compliance with the measures referred to in Article 58, paragraph 2, of the GDPR, insofar as they are previously

with regard to the controller […] in question with regard to the same

matter have been taken;

j. adherence to approved codes of conduct in accordance with Article 40 of the GDPR or of

approved certification mechanisms in accordance with Article 42 of the GDPR; and

k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as

financial gains made, or losses avoided, arising directly or indirectly from the infringement

result.

Pursuant to Article 9, when determining the fine, the AP takes into account, if necessary, the financial

circumstances of the offender. In case of reduced or insufficient carrying capacity of

the offender can further mitigate the fine to be imposed by the AP if, after application of Article 8.1

of the policy rules, determination of a fine within the fine range of the next lower category

in its opinion would nevertheless result in a disproportionately high fine.

4.3

With regard to violations for which the AP can impose an administrative fine of up to the amount

of € 10,000,000 or up to 2% of the total worldwide annual turnover in the previous financial year, if this

figure is higher, the AP has classified the violations into three categories in the 2019 Fine Policy Rules,

to which hefty administrative fines are attached. The fine categories are

fine amount

ranked according to the seriousness of the violation of the aforementioned articles, with category I being the least

serious offenses and category II or III the most serious offences.

Violation of Article 32(1) of the GDPR is classified in Category II, for which a

fine range between € 120,000 and € 500,000 and a basic fine of € 310,000 has been set. the AP

uses the basic fine as a neutral point of departure. The amount of the fine is determined by the AP pursuant to Article 6 of the Fines Policy Rules 2019 on the basis of the factors referred to in Article 7 of the Fines Policy Rules 2019, by decreasing or increasing the amount of the basic fine. It includes to assess (1) the nature, seriousness and duration of the violation in the specific case, (2) the intentional or negligent nature of the infringement, (3) the measures taken to mitigate the damage suffered by data subjects limit damage and (4) the categories of personal data to which the breach relates. In principle, within the bandwidth of the fine category linked to that violation stayed. The AP may, if necessary and depending on the extent to which the aforementioned factors give rise to this apply the penalty bandwidth of the next higher and next lower category, respectively.

4.4

4.4.1 Nature, seriousness and duration of the infringement

Pursuant to Article 7, under a, of the Fine Policy Rules 2019, the AP takes into account the nature, seriousness and the duration of the infringement. In assessing this, the AP takes into account, among other things, the nature, size or purpose of the processing as well as the number of data subjects affected and the extent of the damage suffered by them injury.

Article 32 of the GDPR, read in conjunction with the NEN 7510 and 7513, oblige healthcare providers to: confidentiality and due care with regard to medical data. The importance of meeting appropriate security measures include preserving and restoring the trust of patients in a careful handling of their medical data. Shame on it has no an impact only on the reputation of the healthcare providers involved, but on the entire sector. Security measures, such as measures related to two-factor authentication and the regular checking the log files are necessary measures to preserve and restore data to trust.

The Haga Hospital has in any case not had any appropriate security measures since January 2018 affected by two-factor authentication and the regular review of log files. It hospital information system does not have the built-in obligation - but only the possibility -

to log in with two-factor authentication and she doesn't check the logging regularly. As a result, in

In any case, during this period, the necessary measures have not been taken with regard to the

protection of personal data, in particular measures relating to the prevention and detection

of (possible) unauthorized access to patient records. The violation therefore lasts on a structural basis

manner for a long period of time, during which time a large group of unauthorized persons can access

to obtain health data from patients of the Haga Hospital. All the more in light of the

data breach of the well-known Dutchman, in which the Haga Hospital found at the beginning of 2018 that a

a large number of employees had unauthorized access to a patient file, had it on the road

of the Haga Hospital to meet the standards - which also relate to the prevention of such

unauthorized access - to implement and to detect the violation of Article 32 of the GDPR as soon as possible

to end. In view of this, as well as the large number of patients involved who are

included in the hospital information system29 and the type of personal data (health data),

In the opinion of the AP, there is a situation in which that trust has been betrayed to a great extent.

The AP considers this serious.

Insofar as the period of the detected violation relates to conduct by the Haga Hospital

under the operation of the Wbp, it is important that the Haga Hospital is also governed by the Wbp

- similar to the GDPR regime - appropriate technical and organizational measures should be taken

to protect the personal data.30 A material change in the provision is therefore

no way. Moreover, not complying with the same obligation under the Wbp, albeit with a lower

basic fine than under the GDPR, with the same fine category and corresponding bandwidth

fine. In the opinion of the AP, there is also a serious situation under the Wbp regime

culpable negligence31 on the part of the Haga Hospital, now that the Haga Hospital also in this period has failed to take measures to ensure the correct implementation of the handling of two-factor authentication and checking the log files regularly. From the Haga Hospital may partly in view of the nature and scope of the processing, it is expected that it is aware of the applicable standards. The importance of this is reinforced by the data breach that occurred in January, that can also be prevented and noticed by taking such measures. With this in mind with regard to the duration of the violation, the AP takes into account a period from January 2018 to at present, in which it considers it particularly important that, in the opinion of the AP, this constitutes a structural violation that still continues.

In view of the seriousness of the ongoing violation, the AP sees reason to increase the basic amount of the fine pursuant to Article 7, opening words and under a, of the 2019 Fine Policy Rules, to be increased by € 75,000 to € 385,000.--.

4.4.2 Intentional or Negligent Nature of Infringement

Pursuant to Article 7, under b, of the Fine Policy Rules 2019, the AP takes into account the intentional or negligent nature of the infringement.

In the report “Investigation of illegal access to patient file” prepared by the Haga Hospital of May 2018 it states that a large number of employees have illegally consulted a patient file. They had no treatment or care relationship with the patient. Various measures are recommended, which

29 In this context, the AP refers to the figures from the Annual Report submitted by the Haga Hospital for its opinion hearing. In 2017 Haga Hospital (completed) 28,500 admissions, 158,000 first outpatient clinic visits, 52,000 first aid consultations and 143,000 nursing days.

30 Article 13 of the Wbp, read in conjunction with read in conjunction with Article 3(2) of the Electronic Decree data processing by healthcare providers and the provisions under 9.4.1 and under 12.4.1 of NEN 7510 -2.

31 Article 66(4) of the Wbp, from which it follows that the AP does not impose an administrative fine until after the AP has issued a binding instruction

also see to doing extra random checks to test compliance with the regulation. The management of

As a participating member of the Data Leak Committee, the Haga Hospital was aware of the unauthorized

access to this patient file.32 Reference is made in the Information Security Policy to NEN-7510

and NEN 7513, which must be complied with. Now that the measures taken do not see a correct

implementation of the use of two-factor authentication and regular checking of the

log files, but of the Haga Hospital, partly in view of the nature and scope of the processing

may be expected to ascertain the standards that apply to it, the AP is of the opinion that

Haga Hospital has in any case been particularly negligent in taking such measures.

The AP also takes into account the reaction of the Haga Hospital during the OTP that it is conducting

in connection with follow-up actions due to the aforementioned data breach, did not have time available to take a

security measure that involves regular checking of log files. The Haga Hospital is

responsible for putting in place structures and resources appropriate to the nature and

complexity of the hospital. As such, it cannot legitimize breaches of the GDPR by a deficiency

to claim resources. That the Haga Hospital in connection with the encountering of other

security measures does not have time available, therefore - whatever it is - do not fire her

of the obligation to also take appropriate security measures aimed at preventing the

present continuous violation. Nor is the finding of the Haga Hospital that the aforementioned

data breach, she said, was not a result of the fact that two-factor authentication and the regular

checking log files as proposed in its opinion of 18 April 2019 is not yet complete

implemented. In addition, the AP notes that two-factor authentication and regular checking of

log files, in addition to the others affected by the Haga Hospital as a result of the aforementioned data breach

security measures, see to the prevention and detection of unauthorized access to patient data.

In the light of Article 32, first paragraph, of the GDPR, a series of measures must be taken.

In view of the foregoing, the AP is of the opinion that the Haga Hospital is in any case particularly negligent

been involved in taking appropriate security measures regarding the use of two-factor

authentication and checking the log files regularly.

In view of the negligent nature of the infringement, the AP sees reason to adjust the basic amount of the fine on the basis of

of Article 7, under b, of the Fine Policy Rules 2019 by € 75,000 to € 460,000.

4.4.3 Measures taken

Pursuant to Article 7, under c, of the Fine Policy Rules 2019, the AP takes into account the

controller has taken measures to prevent the damage suffered by data subjects

to limit.

Based on the report “Investigation of illegal access to patient file” of May 2018, the

Haga Hospital recommended a number of security measures on its own initiative. These measures

saw, among other things, the awareness of the employees, the more frequent carrying out of random checks,

inventorying and, where necessary, adjusting the authorizations and tightening the

Authorization policy and the emergency button procedure warning text. The AP has in its final

32 This is apparent from, among other things, p. 4 of the report Investigation of unauthorized access to patient records and the

statement of

[CONFIDENTIAL] Report of conversations OTP Haga Hospital.

March 2019 report concluded that Haga Hospital's access control policy is adequate

to standard NEN 7510-2. The AP has also concluded that the Haga Hospital has taken sufficient measures
has taken with regard to the awareness of employees regarding
information security. In view of this, the AP has assessed that the Haga Hospital at least some
measures recommended in the report regarding the protection of patient data in the
hospital information system of the Haga Hospital.
The downside of this is that the report “Investigation of illegal access to patient records” explicitly states
that more frequent sampling should be done to check log files,
which the Haga Hospital has not (yet) followed up. The reaction of the Haga Hospital during the
OTP that in connection with follow-up actions due to the aforementioned data breach, it did not have time available for the
taking a security measure that involves regular checking of log files, discharges
in view of the foregoing under paragraph 3.3.3, it does not have this obligation. Furthermore, the part sees
authentication par excellence to prevent unauthorized access to patient data. It
Haga Hospital has wrongly failed to pay attention to this on its own initiative, which is all the more
would have been obvious as a result of the aforementioned data breach.
Now that the security measures related to the protection of patient data must be
are considered, the AP sees no reason to change the basic amount of the fine pursuant to Article 7, under c
of the 2019 Policy Rules.
4.4.4 Categories of personal data
Pursuant to Article 7, under g, of the 2019 Fine Policy Rules, the AP takes into account the categories of
personal data to which the infringement relates.
The Haga Hospital processes a large amount of special personal data in the
hospital information system.33 Unauthorized access to patient records can lead to serious adverse
have an impact on the protection of personal data with regard to health.
Now the categories of personal data to which the infringement relates in the present case
also in the assessment of Article 7, first paragraph, opening words and under a, of the Fine Policy Rules 2019 at the
nature and seriousness of the infringement has been included as an increasing fine, the AP sees no reason to

the basic amount of the fine also independently on the basis of Article 7, under g, of the Fine Policy Rules

to increase in 2019.

4.4.5 Other circumstances

The AP sees no reason to increase the basic amount of the fine on the basis of the other provisions in Article 7 of the

Circumstances referred to in the Penalty Policy Rules 2019, to the extent applicable in the present case,

to increase or decrease. Insofar as the Haga Hospital has argued that it cooperated with

the AP's investigation and has immediately drawn up action plans to address the identified by the AP

33 https://www.hagaziekenhuis.nl/about-hagaziekenhuis/reporting-and-accountability/kern Figures.aspx

The number of admissions in 2017 was 28,498, the number of first outpatient clinic visits 158,176 and the number of first aid

consultations 52.2 41.

to improve imperfections, it is important that this cooperation does not go beyond its legal

obligation to comply with Article 32(1) of the GDPR. The AP sees no reason for the judgment that

Haga Hospital has acted in a special way, as a result of which the consequences for the rights of

stakeholders are significantly limited. The AP takes into account that the Haga Hospital - despite the aforementioned

data breach and the AP's announced investigation in October 2018 - has not taken any action since then

taken and actually applied to bring the violation to an end in the short term.

In view of the foregoing, the AP sets the total fine amount at € 460,000.

4.4.6 Proportionality

Finally, on the basis of Articles 3:4 and 5:46 of the Awb (principle of proportionality), the AP assesses whether the

applying its policy for determining the amount of the fine given the circumstances of the

specific case, does not lead to a disproportionate outcome. Applying the principle of proportionality

According to the 2019 Fine Policy Rules, the AP entails that, if necessary, when determining the fine takes into account the financial circumstances of the offender.

During the opinion session, the Haga Hospital invoked limited capacity, substantiated with the draft annual accounts for 2018. In that context, she argues that the Haga Hospital in 2018 [CONFIDENTIAL] as a result of incidental income. The AP does not see any reason to assume that the Haga Hospital will be fined € 460,000 in view of its financial situation position could not bear.

4.4.7 Conclusion

The AP sets the total fine at € 460,000.

5.

5.1

Now that it is a continuous violation of Article 32, first paragraph, of the GDPR, it must be addressed as soon as possible may be terminated. For that reason, the AP imposes an order subject to a penalty in addition to the aforementioned fine on the basis of Article 58, second paragraph, preamble and under d, of the AP, Article 16, first paragraph, of the UAVG and Article 5:32, first paragraph, of the Awb.

5.2

The AP attaches a grace period of fifteen weeks to the order subject to periodic penalty payments. At the determining this period, it has taken into account the planning relating to the intended measures as included in the opinion of the Haga Hospital of 18 April 2019 . ter

The Haga Hospital explained that the implementation of the measures such as included in its planning are in its control and that the planning is realistic. Although the schedule as drawn up by the Haga Hospital, also assumes a check of log files within the

Beneficiary term and amount of penalty payment

Charge under penalty

Cause

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

authorization profile of six (regular or otherwise) patient files and this because of the very limited

size, in the opinion of the AP, in view of the foregoing, does not correspond to the required appropriate

security level, the AP does not see that the Haga Hospital is not within this favorable period

can also comply with Article 32(1) of the GDPR on this point. It is important that the planning

a weekly (manual) check of the logging of all patient files that - outside the

authorization profile - have been consulted through the emergency button procedure. It cannot be seen that they are not

within the beneficiary period also with regard to the checking of log files within the

authorization profile can comply with Article 32(1) of the GDPR. It is not required that the control

of the logging refers to all patient files that have been consulted within the authorization profile, but that

the control is arranged in such a way that cases of unlawful processing that take place

can be sufficiently detected within the authorization. Now the question is whether at this point is

compliance with Article 32, first paragraph, of the GDPR depends on the way in which control takes place -

for example on the basis of a profile of indications that it uses to detect unlawful access

trademarks - and the entirety of security measures should be considered in that context, the AP can de

extent of a required regular check of the log files in advance. It

Haga Hospital must therefore explain how the (intended) check according to Haga Hospital is in

her case contributes to an acceptable level to the detection of unlawful access or use

of patient data within the authorization profiles.

Article 5:32b, third paragraph, of the Awb prescribes that the penalty amounts are in reasonable proportion

to the gravity of the harmed interest and to the intended effect of the penalty. In the latter case

It is important that a penalty payment must provide such an incentive that the order is complied with.

If the Haga Hospital does not end the violation found within fifteen weeks, the

after the end of that beneficiary period for every two weeks that the burden has not been (fully) met

a penalty. The AP sets the amount of this penalty every two weeks after the end of the period

beneficiary term fixed at an amount of € 100,000 (in words: one hundred thousand euros), up to a

maximum amount of € 300,000 in total (in words: three hundred thousand euros).

If the Haga Hospital forfeits the penalty payment immediately after the end of the beneficiary period

wishes to prevent, the AP advises the Haga Hospital to send the documents - with which the Haga Hospital

can demonstrate that it complies with the order subject to periodic penalty payments - on time, but no later than one week

before the end

of the beneficiary period to the AP for assessment.

6. Operative part

fine

Due to violation of Article 32, first paragraph, of the GDPR, the AP submits to the Haga Hospital, read in

connection with Article 3, second paragraph, Decree on electronic data processing by healthcare providers and

the provisions of 9.4.1 and 12.4.1 of NEN 7510-2, an administrative fine in the amount of

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

€460,000 (in words: four hundred and sixty thousand euros).34

Charge under penalty

The Haga Hospital must submit the application within fifteen weeks of the date and with due observance of this decision

within the framework of data processing in the hospital information system of the Haga Hospital,

accessible to its employees, to take measures that lead to:

1. this access is only possible using two-factor authentication;

2. the log files are regularly checked for unauthorized access or use

of patient data.

If the Haga Hospital does not take the measures within fifteen weeks after the date of this decision,

has carried out to (fully) comply with the order, the Haga Hospital forfeits a penalty of

€ 100,000 (in words: one hundred thousand euros) for every two weeks after the end of the

beneficiary period, up to a maximum amount of €300,000 in total (in words: three hundred thousand

euros).

Yours faithfully,

Authority Personal Data,

w.g.

mr. A. Wolfsen

Chair

Remedies Clause

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the

decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. For the

submitting a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Make an objection

against a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority. It

The address for submission on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ Den Haag.

State 'Awb objection' on the envelope and put 'objection' in the title of your letter.

In your notice of objection, write at least:

- your name and address;

- the date of your notice of objection;

- the reference mentioned in this letter (case number); or attach a copy of this decision;

- the reason(s) why you do not agree with this decision;

- your signature.

34 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB).