Registered

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

authoritypersonal data.nl

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

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 Stichting Hagaziekenhuis (Hagaziekenhuis) a

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

2018 to date has not met and does not meet the requirement of two-factor authentication and the

regular review of log files. As a result, it has not taken sufficient appropriate measures

as referred to in Article 32, paragraph 1, 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 pertains 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 (amount of the) administrative fine is elaborated and entered
Chapter 5 shows the order subject to periodic penalty payments. Chapter 6 contains the operative part 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 that has its registered office at Els Borst-Eilersplein 275, (2545
AA) in The Hague. The Haga Hospital was established on July 1, 2004 and is registered in the Chamber of Commerce
Commerce registered under number 27268552. In 2017, the Haga Hospital (rounded off) had a total
28,500 admissions, 158,000 first outpatient visits, 52,000 first aid consultations and 143,000
nursing days.1

Stichting Reinier Haga Groep (hereinafter: RHG) has its registered office at the same address as the
Haga Hospital. 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,
The Langeland Hospital Foundation and the Haga Hospital.

1.2

Process flow

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

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

In response to that report, the AP has sent a written request for information by letter dated 23 April 2018 sent to the Haga Hospital. The Haga Hospital followed this up in a letter dated 15 May 2018 datum.

In response to the information sent by the Haga Hospital, the AP has applied Article 58, paragraph 1, under b, of the AVG decided to conduct further research into, insofar as this applies importance, access to patient data in the digital patient files at Haga Hospital. By letter dated October 12, 2018, the AP sent a written request for information to the Haga Hospital. The Haga Hospital has followed up on this.

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

In a letter dated November 19, 2018, the AP has provided the concise representation of the relevant statements from the employees of the Haga Hospital sent to the Haga Hospital during the OTP with the opportunity to make known the factual (in)accuracy of the statements.

In a 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 the opinion hearing.

2 Report number [CONFIDENTIAL].

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

The results of the further investigation have been 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 in a letter dated 16 January 2019, the Haga Hospital has letter dated 4 February 2019 in response to the Preliminary Findings report.

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

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

Also given the opportunity by letter of April 4, 2019 by the AP, the Haga Hospital has letter dated 18 April 2019, expressed its views in writing on this intention and the implications thereof based final report.

Research background

On April 25, 2019, an opinion hearing took place at the offices of the AP at which the Haga Hospital has also verbally explained its point of view.

In an email dated 30 April 2019, Haga Hospital sent two documents on request.

By letter of 16 May 2019, the AP sent the report of the opinion hearing to Haga Hospital.

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 record will take security measures.

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

consult patient files. In case of doubt, an investigation follows. An investigation into the

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

Scope GDPR

According to the report, (possibly) unlawful access to the patient file to which the data breach relates.3 In the report states that 197 employees, of which 100 unlawfully,4 had access during the period under investigation had in the patient record. The Haga Hospital concludes that the solution is necessary lead to a structural improvement, for which the current and future measures contained therein mentioned must be regularly tested for correct operation and must be changed if necessary adjusted.5

In response to the aforementioned report, the AP decided in October 2018, including further investigation to the security measures of the Haga Hospital.

2. Legal framework

2.1

Pursuant to Article 2, paragraph 1, of the GDPR, this Regulation applies to the whole or in part automated processing, as well as to the processing of personal data contained in a file included or intended to be included therein.

Pursuant to Article 3, paragraph 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 relating to 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”: a […] legal entity that, alone or jointly with others, achieves the purpose of

and determines 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, paragraph 1, of the GDPR, the controller shall take […], taking into account

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

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

3 pg. 3 of the report.

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

5 pg. 7 of the report.

Security Obligation

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

liberties of persons, appropriate technical and organizational measures to prevent one at risk

to ensure an appropriate level of security […].

Pursuant to the second paragraph, the assessment of the appropriate security level takes particular account

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

unauthorized disclosure of or unauthorized 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 Processing of Personal Data Act in the healthcare sector, 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 section 15j, subsection 1, 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 Electronic Data Processing by Healthcare Providers Decree

The Electronic Data Processing by Healthcare Providers Decree is a general measure of board as referred to in Article 15j, first paragraph, of the Additional Provisions for Processing Act personal data in healthcare.

Pursuant to Article 1, the Electronic Data Processing Decree means by healthcare providers below:

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

“NEN 7513”: further interpretation of NEN 7510 regarding the recording of actions on electronic 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 for 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 is responsible for a care 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 does

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 concerns, among other things, logging. In NEN 7510 and 7513

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

It is important 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 requirements), paragraph 5.1 (General) of NEN 7513 states that the logging in the

should generally make it possible to irrefutably determine which events occurred afterwards

occurred on a patient file. To this end, all systems that contain data must

form part of a patient record, and at least keep records of:

- which event took place;

- date and time of the event;

- which client it concerned;

- who the user was;

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

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

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

log user activities, exceptions and information security events

are created, stored and regularly reviewed.

2.3

Pursuant to Article 58, paragraph 2, opening words and under d and i, in conjunction with Article 83, paragraph 4, opening words and

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

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

take 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. depending on the circumstances of each case, in addition to or instead 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]

Judgement

Pursuant to Article 83, paragraph 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 each case.

Pursuant to paragraph 2, administrative fines shall be imposed, depending on the circumstances of the

specific case, imposed in addition to or instead of the provisions referred to in Article 58, paragraph 2, under a to h and under j,

referred measures.

It follows from the fourth paragraph, preamble and under a, that a breach of the obligation of the

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

administrative fine of 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 Implementation Act (UAVG)

Pursuant to Article 14, third paragraph, 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

amounts mentioned.

3.

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

explained who can be regarded as the controller for which processing. The

violation of article 32, first paragraph, of the AVG, 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 determined 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 on 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, is used by Haga Hospital to store data relating to patients

included. Therefore, there is a 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 leak and the notification by the Haga Hospital to the AP on April 4, 2018, the

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

GDPR became applicable7 and the UAVG entered into force.8

In response to the aforementioned data leak and the report drawn up for this purpose by the Haga Hospital

“Final Report Investigation Unlawful Access to Patient File” of May 2018, the AP has in October

Authority AP

6 Article 51 of the UAVG.

7 Article 99, second paragraph, 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 - a further investigation into

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

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

staff. The research focused, among other things, on whether the The Hague-based

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

hospital information system comply with - the current - article 32 of the AVG. The AP

with regard to the violation established in the final report pursuant to Article 58, paragraph 2,

preamble and under d and i, in conjunction with article 83, fourth paragraph, preamble and under a, of the AVG and article

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

payments,

if circumstances warrant it.

3.2 Controller

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

3.2.1

As also confirmed by the Haga Hospital at the hearing, the general part of the by RHG established Information Security Policy applies to all data processing in all RHG business addresses, including the Haga Hospital.10 When applying information security within RHG, the standards NEN 7510 and NEN 7513 are used as a starting point used.11 These standards are not further elaborated 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 interpretation of the general part - which can differ per organization within RHG - is included in the appendices to the Information Security Policy. Appendix 2 refers to the local implementation by the Haga Hospital. The Haga Hospital has its own Information Security Officer (ISO), who checks it on a daily basis Information Security Policy

9 https://www.hagaziekenhuis.nl/over-hagaziekenhuis/goed-om-te-know/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]

point of contact for all information security matters within that hospital and the local

coordinates information security activities.13 All parts of RHG must

have taken adequate measures to ensure the continuity of the operational activities

secure. The management of - among other things - an emergency button procedure forms part of this.14 The

standards NEN 7510 and NEN 7513 are not further discussed in Annex 2 (Local implementation Haga Hospital).

worked out.

3.2.2 Authorization Policy

The Authorization Policy has been drawn up by the Haga Hospital and contains policy for the establishment and

systems related to 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 for the processing of

personal data are 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. The Haga Hospital has explained that at the hearing

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 broad provisions that pertain to the processing of

personal data. The Privacy Statement contains further details of the Privacy Regulations, based on

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 control and promotion of the care provision.

The Privacy Statement also states that Haga Hospital also collaborates with others

healthcare institutions. The Haga Hospital asks the patient's permission before starting the treatment in question

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 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 differs per hospital and it becomes general

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 Board.18

3.2.5 Assessment 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. She decides 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 states the purposes of data processing determined by the Haga Hospital.

For the question of whether the Haga Hospital makes decisions alone or together with RHG with regard to the determination of purposes and means of data processing in the hospital information system the Haga Hospital, it is important that RHG only has a general information security policy and a General Privacy Regulations. This adopted general policy does not cover the level of detail 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, first paragraph, 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. It falls further partnership outside the scope of the Authorization Policy - which pertains to 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 of [CONFIDENTIAL] of the Haga Hospital, the AP is with due observance of the foregoing is of the opinion that the Haga Hospital independently has the formal legal authority has to determine the purposes and means of data processing in the hospital information system of the Haga Hospital.

3.2.6 Conclusion

Now that the Haga Hospital is in the opinion of the AP with regard to the hospital information system

autonomous, the Haga Hospital - and not also RHG - with regard to

data processing operations in that hospital information system as controller as intended

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 being infringed

Introduction

18 pg. 2 of the Record of interviews OTP Haga Hospital.

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

assess inherent risks and take measures to mitigate risks. That

measures must ensure an appropriate level of security, taking into account the state

of the technique and the implementation costs compared to the risks and the nature of the protection

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

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

Appropriate security measures help maintain patient confidence

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 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 dedicated to processing sensitive information

information, the controller must at least use two-factor authentication, in order to

establish the identity of users. Furthermore, log files of events that

record user activities, exceptions and information security events

created, stored and reviewed regularly. The foregoing follows from NEN 7510 -2, in which

security standards have been included that pertain to a further interpretation of Article 32 of the GDPR

concerns information security in healthcare, referred to in 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 that

process health information, should be able to establish the identity of users. This should

be done through authentication involving at least two factors. This

means the identity of the user to access the health information system

for example, is determined on the basis of knowledge (code or a password) and possession (employee pass).

Regulations Personnel Card and User Manual Virtual Workplace

The Staff Pass Regulations of the Haga Hospital20 state that all employees of the

Haga Hospital have a staff pass that can be used to log in to the computers. The

The powers of this own identity card are related to the function and workplace of the

colleague. This pass can prevent other users from accessing confidential documents

can see. Logging in is also possible without a pass, but using username and

password. The pass is for convenience only, according to the Scheme.

The Virtual Workplace User Manual21 confirms that the workstations have a card reader

are suitable for virtual work. Employees can manually, but after registration also with the

19 Recital 83 of the GDPR.

20 Revision date 13 June 2017.

21 of August 14, 2018.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

register a personnel card.22

Declaration Haga Hospital

During the OTP on October 31, 2018, Haga Hospital confirmed that there are two ways to
are logged into the computers and the hospital information system. One of the options is with
using the staff pass, 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 linked to this personal network account. This means that if one
employee once logged in to the VDI, this employee also has access to it
hospital information system. The user can then use it for four hours - the so-called 'grace
period'- on any workstation with the card log off and on without entering a user name,
password and/or pin code. The other option is without using the staff pass,
where you can manually log in to the VDI with a user name and password. Once
logged in, the employee also has access to the
hospital information system.23

View

The opinion of the Haga Hospital 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 hearing it was explained that the Haga Hospital started the virtual one in 2012
workplaces, also with the option to log in manually. She has set herself the goal of
October 1, 2019 to have implemented permanent two-factor authentication hospital-wide, whereby
the option to log in via one-factor authentication disappears. Furthermore, the Haga Hospital will de

abolish the so-called 'grace period', so that access via two-factor authentication requires a

PIN code will be requested.

Rating AP

Now that the user authentication strength 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 establishes - and does not adjust either

dispute - 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 pass, authentication takes place on the basis

of a user name 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 be thus

take place solely on the basis of knowledge (code or a password), without possession (employee pass).

Therefore, a single method of consultation of the hospital information system by the

not exclude 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 hearing.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

pursuant to Article 32 of the GDPR, read in conjunction with Article 3, paragraph 2, Electronic Decree

data processing by healthcare providers and the provisions under 9.4.1 of NEN 7510-2.

3.3.3 Reviewing Log Files Regularly

Healthcare institutions must keep track of who has consulted which patient file and when

(logging) and this should be checked regularly. In this way, the setting can be unauthorized
signal access and take measures. This is based on paragraph 12.4.1 of NEN 7510-2, in which
states that event logs that include user activities, exceptions, and
record information security events should be created, retained and regularly updated
be assessed.
With reference to the report “Access to digital patient records within healthcare institutions” of
June 2013, the starting point of the AP24 is that checking the logging must be systematic and consistent
take place, whereby a random check and/or check based on complaints is not sufficient
is. It is important in this respect that a random random check does not involve a
system aimed at unlawful use and risks.
Authorization Policy
The Authorization Policy of the Haga Hospital states that security and logging in accordance with the
principles 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 unauthorized 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 specialties and (3)
patient files that have been accessed via the so-called emergency button procedure, also known as
referred to as the 'breaking the glass' procedure, described in more detail below.25
Pursuant to the Authorization Policy, the DPO serves for (1) the regular patient files once every two
months to audit access to the system in accordance with the established authorization procedure.
At the opinion hearing, Haga Hospital explained that this should be understood as a
checking one patient file every two months. The Haga Hospital has further explained that (2)
if a selected file belongs to treatment in the specialisms psychiatry, psychology, VIP,
own personnel 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 of time.

Employees of the Haga Hospital can also use (3) an emergency button procedure,

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

is. The procedure does not involve searching for such patient data and actually wanting to view it

of this data will see a message on the screen, informing employees that they cannot

are authorized to access this specific patient data. To the employees

24 It is true that it falls within the scope of the Wbp, but the purport of article 32 of the AVG is different from article 13 of the

time

applicable Wbp not changed.

25 pg. 3 of the Authorization Policy.

asked to provide a reason why access is nevertheless necessary. Using that procedure

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

Authorization policies state that a failed access attempt as well as successful access to a digital

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

to be checked for legality.

Declaration Haga Hospital

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

checks on the logging are carried out by the ISO and the FG. It was the first check in 2018

patient file of the well-known Dutchman, given the large amount of access to this specific

dossier.26 At the request of patients and employees, the Haga Hospital will have more checks in 2018

performed, and no irregularities were found. [CONFIDENTIAL] further stated

that the Haga Hospital intends to conduct six random samples per year in 2019 as part of an audit

of the logging in accordance with the Authorization Policy, whereby six different patients of
different departments will be checked. Due to the busyness due to the aforementioned data breach
and the follow-up actions to this, at the time of the statement of 31 October 2018, Haga Hospital was (still)
didn't get 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 a sample basis
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
per logging line it is determined whether the person who logs in is part of the treatment team of the
concerning patient. Upon request, the Haga Hospital has a rough estimate for the opinion hearing
made of the scope of the audit trail, which consists of five steps. The first three steps are possible
are carried out by one employee and see to the generation of the logging, the completion and
checking and determining the treatment team. Further research takes place in the last two steps
place, performed by several employees. The execution 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
covers, according to the Haga Hospital. With regard to the monitoring 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
checking logging. The systematic analysis (3) includes a weekly check of the logging
of all patient records consulted via the emergency button procedure. The one she drafted
planning aimed at October 1, 2019 assumes a manual check. The possibilities of using
[CONFIDENTIAL] - as a technical aid for checking the logging
still being investigated by the Haga Hospital.

At the hearing, the Haga Hospital confirmed that in the period from January 2018 up to and including

26 See also the response from Haga Hospital dated 4 February 2019.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

October 2018 proactive one check on logging with regard to the file of the well-known Dutchman and six logging checks related to six patient and staff request records has performed. After October 2018, various checks at the request of patients and / or employees occurred. In January 2019, Haga Hospital started with the first sample of the planned six samples per year. The second study is for April/May 2019 on the planning, according to the Haga Hospital.

Rating AP

The AP notes that in 2018 the Haga Hospital - with the exception of one proactive sample - only in response to a few complaints and requests. The one done in 2019 proactive monitoring (involving up to two patient records) does not also include a separate one checking the logging of patient files that have been consulted via the emergency button procedure. It Haga Hospital has therefore at least during the aforementioned period (January 2018 to the present) not acted in accordance with its own Authorization Policy. Aside from that, doing just one or a few proactive sample(s) per year amply and evidently insufficient to be able to speak of an appropriate security level that pertains to signaling unauthorized access to patient data and taking measures in response to unauthorized access. In doing so, the AP important the scale of the processing of health data by the hospital27 and the lack of regular checks on the use of the emergency button procedure, as a result employees can access more data than they are initially authorized to are. In view of this, there are no appropriate measures with regard to checking the logging, such as

is 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 periodic penalty payments, the AP also answers the question of whether the

Authorization policy provides for a systematic, consistent control of the data from the logging. The

AP has established, partly on the basis of the explanation of the Haga Hospital, that the Authorization Policy

provides for a check on the logging of six (regular or not) patient files and a regular

control of patient records to which access has been obtained using the

emergency button procedure. What should be understood by regular checks of the latter files,

is not further elaborated in the Authorization Policy. In the view of the Haga Hospital van

April 18, 2019 states that it aims to review all patient files weekly by October 1, 2019 at the latest.

studies that were consulted via the emergency button procedure. The Haga Hospital is committed to the

implementation of the proposed 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 AP's opinion, such a weekly check is absolutely sufficient

the requirement of systematic, consistent control of the data from the logging. However, this is late

without prejudice to the fact that the Haga Hospital also bears the risk of abuse within the authorization profile

27 In this context, the AP refers to the figures from the annual report submitted by the Haga Hospital for the opinion hearing. In

2017

the Haga Hospital (rounded) 28,500 admissions, 158,000 first outpatient visits, 52,000 first aid consultations and 143,000

nursing days.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

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 what health data. On a volume of - in 2017 - (rounded) 28,500 admissions, 158,000 first outpatient clinic visits, 52,000 emergency room consultations and 143,000 nursing days, provides a control of six patient files annually insufficient effort to resolve cases of unlawful processing take place within the authorization to a sufficient extent. In the opinion of the AP does this therefore not lead to the required appropriate level of security in cases where the file falls within the authorization has been consulted.

The current state of the art is indicative of what constitutes appropriate measures in the sense of Article 32, first paragraph, of the GDPR can be considered. The Haga Hospital has no plausibility made that - possibly besides [CONFIDENTIAL] - no other technical support options are available. The steps taken by the Haga Hospital to come an update in that context are therefore recommended. Insofar as the Haga Hospital has no or limited technical support to perform or support logging control, as it has put forward in the opinion, it should organize the control of the logging. 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 cannot be seen that a manual checking the logging of more than six files - not consulted via the emergency button procedure - per years, cannot be required of her. That the Haga Hospital, as she has a viewpoint hearing explained, also takes preventive measures with a view to preventing unauthorized access to patient data, which, among other things, pertains to 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.

Considering that the Authorization Policy, among other things, provides for a check of one sample of one file every two months, in the AP's opinion, that policy does not provide for a systematic, consistent monitoring of the logging.

3.3.4 Conclusion

In view of the foregoing, the AP is of the opinion that the Haga Hospital is subject to Article 32, paragraph 1, of the GDPR, read in conjunction with Article 3(2) of the Electronic Data Processing Decree care 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 and the regular review of log files. The violation is currently ongoing.

4.

4.1

The security measures taken by the Haga Hospital do not concern a (correct) implementation of using two-factor authentication and regularly checking the log files. From the

Haga Hospital may, however, be expected to ascertain the standards that apply to it. Not using two-factor authentication in case of access to patient data - in which section 9.4.1 of NEN 7510-2 leaves no room - and only checks it proactively in practice of the logging of one or more patient records during a period of more than one year, is to the opinion of the AP - and contrary to what the Haga Hospital puts forward - is evident and structural contrary to article 32, first paragraph, of the AVG, read in conjunction with the provisions under 9.4.1 and under 12.4.1 of NEN 7510-2. That the Haga Hospital has argued at the hearing that the standard in 12.4.1 of NEN 7510-2 contains an open standard, this - whatever the case may be - does not alter that, now that the

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

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

12.4.1 of NEN 7510-2. In the present case, the AP sees reason to make use of it

authority to impose a fine pursuant to Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph,

of the AVG, read in conjunction with Article 14, third paragraph, of the UAVG, to the Haga Hospital at

lay.

4.2

Pursuant to Article 58, second paragraph, opening words and under i and Article 83, fourth paragraph, of the GDPR, read in

connection with Article 14, third paragraph, of the UAVG, the AP is authorized to contact 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 Fining Policy Rules 2019 regarding the implementation of the aforementioned power to

imposing an administrative fine, including determining the amount thereof.28

Pursuant to Article 2, under 2.1, of the Fining Policy Rules 2019, the provisions regarding violation

of which the AP can impose an administrative fine not exceeding € 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, classified in Annex 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 legal

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 (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 base fine is

increased or decreased depending on the extent to which the factors referred to in Article 7 are used

give rise.

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

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

Policy rules referred to under a to k:

a. the nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the

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

injury;

b. the intentional or negligent nature of the breach;

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

limit damage;

d. the extent to which the controller […] is responsible in view of the technical and

organizational measures he has implemented in accordance with Articles 25 and 32 of the GDPR;

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

f. the degree of cooperation with the supervisory authority to remedy the breach and

limit the possible negative consequences thereof;

g. the categories of personal data affected by the breach;

h. the manner in which the supervisory authority became aware of the breach, 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, second paragraph, of the GDPR, insofar as they are earlier

in respect of the controller […] in question in relation 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, which may or may not result directly from the breach

result.

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

circumstances in which the offender finds himself. In case of reduced or insufficient capacity of

the offender can further moderate 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 lead to a disproportionately high fine.

4.3

In respect of violations for which the AP can impose an administrative fine not exceeding 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 divided the violations into three categories in the 2019 Fining Policy Rules,

which are associated with mounting administrative fines. The penalty categories are

Fine amount

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

contains serious violations and category II or III contains the most serious violations.

Violation of article 32, paragraph 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 agreed by the AP pursuant to Article 6 of the Fining Policy Rules 2019 then based on the factors referred to in Article 7 of the Fining Policy Rules 2019, by reducing or increasing the amount of the basic fine. It includes, among other things for an assessment of (1) the nature, seriousness and duration of the violation in the specific case, (2) the intentional or negligent nature of the breach, (3) the measures taken to remedy 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 can, if necessary and depending on the extent to which the aforementioned factors give cause to do so apply the penalty bandwidth of the next higher or the next lower category respectively.

4.4

4.4.1 Nature, seriousness and duration of the breach

Pursuant to Article 7, under a, of the Fining 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 size 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 AVG, read in conjunction with NEN 7510 and 7513, obliges healthcare providers to confidentiality and due diligence with regard to medical data. The importance of meeting appropriate security measures include maintaining and restoring trust the patients in careful handling of their medical data. Shaming it does not only an impact on the reputation of the healthcare providers involved, but on the entire sector. Security measures, such as measures related to two-factor authentication and regular checking the log files, are necessary measures for preservation and recovery of that to trust.

The Haga Hospital has had no appropriate security measures since January 2018

impacted on two-factor authentication and regular review of log files. It
hospital information system does not have the built-in obligation - only the possibility -
to log in with two-factor authentication and she does not check the logging regularly. As a result, are in
in any case, during this period, the necessary measures have not been taken that relate to the
protection of personal data, in particular measures related to prevention and noticing
of (possible) unauthorized access to patient records. The violation therefore lasts on a structural basis
continue for a long period of time, during which a large group of unauthorized persons can gain access
access to health data of patients of the Haga Hospital. All the more so in light of it
data leak of the well-known Dutchman, in which the Haga Hospital found at the beginning of 2018 that a

large number of employees have had unauthorized access to a patient file, had it on the road
of the Haga Hospital is based on the standards - which also concern the prevention of such
unauthorized access - to implement and promptly rectify the violation of Article 32 of the GDPR
to end. In view of this, as well as the large number of affected patients who are
included in the hospital information system29 and the type of personal data (health data),
In the AP's opinion, this is a situation in which that trust has been greatly betrayed.
The AP considers this serious.
Insofar as the period of the observed violation relates to behavior of Haga Hospital
under the scope of the Wbp, it is important that the Haga Hospital also falls under the regime of the Wbp
- equivalent to the GDPR regime - appropriate technical and organizational measures had to be taken
take to secure the personal data.30 A material change to the provision is therefore
no way. Moreover, non-compliance 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
fineable. The AP is also of the opinion that there are serious breaches 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 proper implementation of the handling of
two-factor authentication and checking the log files regularly. From the Haga Hospital is allowed
partly in view of the nature and scope of the processing, it is expected that 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. Considering this
with regard to the duration of the violation, the AP takes into account a period from January 2018 up to and including
present, in which it considers it particularly important that, in the opinion of the AP, this constitutes a
structural violation that still persists.
In view of the seriousness of the ongoing violation, the AP sees reason to set the basic amount of the fine
pursuant to Article 7, preamble and under a, of the Fining Policy Rules 2019 to be increased by € 75,000 to
€385,000.

4.4.2 Intentional or negligent nature of the breach

Pursuant to Article 7, under b, of the Fining Policy Rules 2019, the AP takes into account the intentional or
negligent nature of the infringement.
In the report “Investigation into unlawful access to patient files” prepared by Haga Hospital
May 2018 states that a large number of employees consulted a patient file unlawfully.
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 the opinion hearing. In 2017
the Haga Hospital (rounded) 28,500 admissions, 158,000 first outpatient visits, 52,000 first aid consultations and 143,000 nursing days.

30 Article 13 of the Wbp, read in conjunction with Article 3, paragraph 2, 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.

31 Article 66, paragraph 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

unless the violation was committed intentionally or resulted from grossly culpable negligence.

also see to doing additional 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 person

access to this patient file.32 The Information Security Policy refers to NEN-7510

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

implementation of using two-factor authentication and regularly checking the

log files, but of the Haga Hospital, also 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

the Haga Hospital was in any event particularly negligent in taking such measures.

In doing so, the AP also takes into account the reaction of Haga Hospital during the OTP it is taking

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 through a deficiency

to claim resources. That the Haga Hospital in connection with the encounter of others

security measures does not have time available, therefore do not release it - whatever the case may be

of the obligation to also take appropriate security measures to prevent the

current ongoing violation. Neither does the finding of the Haga Hospital that mentioned above

according to her, the data breach was not due to 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, to prevent and notice unauthorized access to patient data.

In the light of Article 32(1) of the GDPR, a set of measures must be taken.

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

has been involved in taking appropriate security measures related to the use of two factors

authentication and regular checking of the log files.

In view of the negligent nature of the infringement, the AP sees reason to base the basic amount of the fine

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

4.4.3 Measures taken

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

measures taken by the controller to mitigate the damage suffered by the data subjects

to limit.

On the basis of the report "Investigation into illegal access to patient records" 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 employees, more frequent sampling,

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

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

32 This is apparent from p. 4 of the report Investigation of illegal access to patient files and the statement of

[CONFIDENTIAL] Report of conversations OTP Haga Hospital.

Date

June 18, 2019

Our reference

[CONFIDENTIAL]

report of March 2019 concluded that the access control policy of the Haga Hospital is satisfactory
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 with regard to
information security. In view of this, the AP has assessed that the Haga Hospital has at least some
measures recommended in the report for the protection of patient data in the
hospital information system of the Haga Hospital.
The flip side of this is that the report explicitly states “Investigation into illegal access to patient files”.
that more frequent random checks should be carried out to check log files,
which Haga Hospital has not (yet) followed up on. The reaction of the Haga Hospital during the
OTP that in connection with follow-up actions due to the aforementioned data breach, it had no time available for it
taking a security measure that involves regularly checking log files
in view of the foregoing under paragraph 3.3.3, it is not of this obligation. Further see the part
authentication par excellence to prevent unauthorized access to patient data. It
Haga Hospital wrongly did not pay attention to this on its own initiative, which is all the more so
would have been obvious as a result of the aforementioned data breach.
Now the security measures that pertain to the protection of patient data as a whole should be
are considered, the AP sees no reason to set 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 Fining Policy Rules 2019, the AP takes into account the categories of
personal data to which the breach relates.
The Haga Hospital processes a large amount of special personal data in the
hospital information system.33 Unauthorized viewing of patient files can have serious adverse effects
impact on the protection of personal health data.
Now the categories of personal data to which the breach relates in the present case
also in the assessment of Article 7, first paragraph, opening lines and under a, of the Fining Policy Rules 2019 at the

nature and seriousness of the infringement has been included as a fine-increasing factor, the AP sees no reason to do so the basic amount of the fine also independently pursuant to Article 7, under g, of the Fining Policy Rules 2019 increase.

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 Fining Policy Rules 2019, insofar as applicable in the present case, to increase or decrease. Insofar as Haga Hospital has argued that it cooperated with the investigation by the AP and has drawn up immediate action plans to address the problems identified by the AP

33 https://www.hagaziekenhuis.nl/over-hagaziekenhuis/verslaglegging-en-verresponsing/kernnummers.aspx The number of admissions in 2017 was 28,498, the number of first outpatient visits 158,176 and the number of first aid consultations 52.2 41.

imperfections, it is important that this cooperation does not go beyond what is legal obligation to comply with Article 32, first paragraph, of the GDPR. The AP sees no reason to rule that the Haga Hospital has acted in a special way, which has consequences for the rights of stakeholders are significantly limited. The AP includes that the Haga Hospital - despite the aforementioned data leak and the investigation announced by the AP in October 2018 - has not taken any measures since then taken and actually applied to end the violation in the short term.

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

4.4.6 Proportionality

Finally, the AP assesses whether the application of 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 means, according to the Fining Policy Rules 2019, that the AP, if necessary, when setting the fine takes into account the financial circumstances of the offender.

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

4.4.7 Conclusion

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

5.

5.1

Since it concerns a continuous violation of Article 32, first paragraph, of the GDPR, this should be done as soon as possible possible to be terminated. For that reason, the AP imposes an order subject to periodic penalty payments in addition to the aforementioned fine on the basis of Article 58, second paragraph, opening lines 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 In determining this term, it has taken into account the planning that pertains to the intended measures as included in the opinion of the Haga Hospital of 18 April 2019 . Ter opinion hearing, the Haga Hospital explained that the implementation of the measures such as included in its planning are in its power 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 Favorable period and penalty amount

authorization profile of six (whether or not regular) patient files and this because of the very limited
size, in the opinion of the AP, in view of the foregoing, is not appropriate to the requirement
security level, the AP does not see that the Haga Hospital is not within this grace period
can also comply with article 32, paragraph 1, of the AVG 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 - are accessed via the emergency button procedure. It cannot be seen that they are not
within the beneficiary period also with regard to the control of log files within the
authorization profile can comply with Article 32, first paragraph, of the GDPR. It is not required that the control
of the logging relates 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 take place
within the authorization can be sufficiently detected. Now the question is whether at this point
compliance with Article 32(1) 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 unauthorized access
trademarks - and the entirety of security measures should be viewed in that context, the AP can de
extent of a required regular check of the log files cannot be indicated in advance. It
Haga Hospital must therefore explain how the (intended) check is carried out according to Haga Hospital
its 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 stipulates that the penalty amounts must be in reasonable proportion

to the seriousness of the violated interest and to the intended effect of the penalty. At that last one

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

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

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

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

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

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

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

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

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

before the end

of the beneficiary period to the AP for assessment.

6. Operative part

Fine

The AP informs the Haga Hospital, due to violation of Article 32, first paragraph, of the AVG, read in

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

the provisions under 9.4.1 and under 12.4.1 of NEN 7510-2, impose 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

Load under duress

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

the context 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 with the application of 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 of the date of this decision

has performed to (fully) comply with the order, the Haga Hospital will forfeit 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 for Personal Data,

e.g.

Mr. A. Wolfsen

Chair

Remedies Clause

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

decides 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 Objection

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

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

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

Write in your notice of objection at least:

- your name and address;

- the date of your objection;

- the reference referred to in this letter (case number); or enclose a copy of this decision;

- the reason(s) why you disagree with this decision;

- your signature.

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