Access to digital

patient files

employees of it

Haga Hospital

Research report

March 2019

Final Report 2019

Table of contents

Resume

When patients visit a hospital for treatment, they must be able to trust that there is
their personal data is treated confidentially and that measures have been taken to
prevent employees who have no treatment relationship with the patient or who do not need the data
for the management of the care provision or treatment, unauthorized in the
view personal (medical) records. In case there is a leak of your personal
data, as a patient you want the hospital to report this to you and to the supervisor.

In October 2018, the Dutch Data Protection Authority (AP) investigated the measures it
Haga Hospital has taken steps to ensure that personal data in the digital patient file is not
be accessed by unauthorized employees. In doing so, the AP has assessed whether those measures are 'appropriate'.
are as referred to in Article 32, first paragraph, opening words, of the General Data Protection Regulation (GDPR).
When testing the security measures taken against Article 32 of the AVG, the NEN 7510 and 7513 are considered
measuring instrument used.

The AP also has the policy of the Haga Hospital with regard to identifying and reporting data leaks
examined (Articles 33 and 34 GDPR).

The AP finds that the Haga Hospital has not taken sufficient appropriate measures in this regard
of the security aspects 'authentication' and 'checking the logging'. The Haga Hospital acts on this basis
contrary to Article 32, first paragraph, opening words, of the AVG.

With regard to the investigated security aspects 'authorisations', 'logging of access' and
'Awareness of employees with regard to information security', the AP finds no violations.

The Haga Hospital has an internal data breach register; data breaches are registered therein,
even if reporting to the AP and to those involved is not necessary. The AP concludes that the written policy of
the Haga Hospital with regard to the registration and reporting of data leaks is in accordance with
Articles 33 and 34 of the GDPR and that Article 24, second paragraph, of the GDPR is complied with on this point.

1 Introduction

1.1 Background and purpose of the research

The reason for the investigation is a report of a data leak from the Haga Hospital on April 4, 2018.
concerns a data breach in which Haga Hospital has established that 85 of its employees have received medical
viewed data of a patient when he was admitted to the Haga Hospital, without doing so
competent, that is to say: without being directly involved in the treatment of the person in question
patient and/or were involved in the administrative handling thereof. The patient was known
Dutchman. In mid-April 2018, various reports appeared in the media about this.
The hospital has announced measures after questions from the Dutch Data Protection Authority (AP).1 This
report contains the results of the further investigation into the security measures of the
Haga Hospital. The research focuses on the situation in October 2018.
The main question in this research is the following:
Are the measures taken by Haga Hospital to ensure that personal data
in the digital patient file cannot be viewed by unauthorized employees, 'appropriate' as referred to in
article 32 of the GDPR?
The AP has investigated the following aspects in this context: authentication, authorisations, logging, control
of the logging and the awareness of employees.
The AP has also investigated the procedures for reporting data leaks (article 33, first
paragraph, and Article 34, paragraph 1, of the GDPR).

1.2 Study progress

In a letter dated October 12, 2018, the AP conducted a further investigation and asked questions. The requested
information was provided by letter dated 23 October 2018 from Haga Hospital.
On October 31, 2018, four employees of the AP conducted an on-site investigation at the
Haga Hospital, Leyweg location in The Hague, where the hospital information system has been examined and

oral statements were also taken from [CONFIDENTIAL].

On November 19, 2018, AP submitted the statements in writing to Haga Hospital. It

Haga Hospital responded in writing to this on 29 November 2018.

On January 16, 2019, the AP sent the preliminary findings to Haga Hospital. It

Haga Hospital responded in writing on February 4, 2019.

1 Following the report of the data breach, the AP requested the Haga Hospital on 23 April 2018 for information regarding the data breach and the measures taken. This information was provided to the AP by letter dated 25 May 2018.

1.3 Legal framework

The data breach took place in January 2018, when the Personal Data Protection Act (Wbp) was still in force

was applicable. As of May 25, 2018, the General Data Protection Regulation (GDPR) is applicable,

as well as the GDPR Implementation Act (UAVG). The Wbp was also repealed on that date, pursuant to Article 51 of the UAVG.

The AP's investigation at Haga Hospital focuses on the situation in October 2018; that is, after

the GDPR becoming applicable.

Lawfulness of data processing

For employees of healthcare institutions, access to personal data about health is in digitized form

patient files only lawfully if and insofar as an employee is directly involved in the

treatment of or care provided to a patient and/or in the management of this

treatment/care provision and access is limited to the data necessary for the

performance of the employee's duties. Incidentally, the personal data may only be

processed by persons who by virtue of their office, profession or statutory regulation or pursuant to a

confidentiality agreement is required. This follows from the provisions of Article 9 of the GDPR, paragraph 2

under h2 and paragraph 33, article 30 of the UAVG, paragraph 3 under a4 and paragraph 45, and article 7:457 first and

second paragraph Civil

Code (BW).6

2 “the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the
the employee's fitness to work, medical diagnoses, the provision of health care or social services or
treatment or the management of healthcare systems and services or social systems and services, under Union law
or Member State law, or under a contract with a healthcare professional and subject to those mentioned in paragraph 3
conditions and guarantees;”

3 “The personal data referred to in paragraph 1 may be processed for the purposes referred to in paragraph 2(h) where
data are processed by or under the responsibility of a professional authorized under Union or Member State law
is bound by professional secrecy by law or by rules adopted by national competent authorities, or by another
person who is also authorized under Union or Member State law or under rules laid down by national competent authorities
secrecy is kept.”

4 “In view of Article 9(2)(h) of the Regulation, the prohibition on processing health data does not apply
applies if the processing is carried out by:

a.

care providers, institutions or facilities for health care or social services, insofar as the
processing is necessary for the proper treatment or care of the data subject or the management of the data subject
relevant institution or professional practice;”

5 “If application is made to the first, second or third paragraph, the data will only be processed by persons from
by virtue of office, profession or statutory regulation or pursuant to a confidentiality agreement. If the
controller processes personal data and does not already rely on him by virtue of his office, profession or law
regulation is subject to a duty of confidentiality, he is obliged to maintain the confidentiality of the data, except insofar as the
law requires him
communication is mandatory or the need arises from his task that the data be communicated to others who are authorized by
virtue of the
first, second or third paragraph are authorized to process it.”

6 “1. Without prejudice to the provisions of Article 448, paragraph 3, second sentence, the care provider shall ensure that

persons other than the patient are not

information about the patient or access to or copies of the documents, referred to in Article 454, are then provided with patient's consent. If provision takes place, this will only take place insofar as this affects personal privacy of another is not harmed. The provision may take place without observing the restrictions referred to in the previous sentences, if required by or pursuant to the law.

2. Others than the patient do not include those who are directly involved in the implementation of the treatment agreement and the person who acts as a replacement for the care provider, insofar as the provision is necessary for the activities to be performed by them in that context."

Security measures to be taken

Article 32, paragraph 1, opening words, of the GDPR stipulates that the controller must use appropriate technical and organizational measures to ensure a level of security tailored to the risk for the data subject guarantees. In doing so, the controller takes into account the available technology and the implementation costs and with the nature, scope, context and purposes of the processing.

The 'Decree on electronic data processing by healthcare providers' contains further rules, among other things established on functional, technical and organizational measures for electronic data processing by healthcare providers. Pursuant to Article 3, paragraph 2, and Article 5, paragraph 1 of the Decision, a healthcare provider must act with regard to the security and logging of its healthcare information system in accordance with the provisions of NEN 7510 and NEN 7513.7,8 The NEN 7510 and NEN 7513 standards contain thus a mandatory further interpretation of Article 32 of the AVG with regard to a safe and careful use of the healthcare information system of the healthcare provider. That is why the AP uses the provisions in NEN 7510 and NEN 7513 as a standard for the assessment of 'appropriate technical and organizational measures".

The following requirements from NEN 7510 and NEN 7513 are involved in the assessment of the appropriate level of the measures taken by the hospital with regard to access to data

electronic patient records:

- The identity of users is established on the basis of two-factor authentication.9

-

-

There is an access control policy for granting access to information.10

Log files are created to irrefutably determine which events happened afterwards

have taken place on a patient file.11,12

- The log files are checked regularly for indications of unauthorized access or

unlawful use of personal data.13

- Employees are made aware of their responsibilities in the field of

information security.14

These standards are further elaborated in Chapter 2 of this report.

Reporting data breaches

Articles 33 and 34 of the GDPR contain the 'obligation to report', which is known in common parlance

data leaks', the obligation to report a personal data breach to the

supervisory authority and the data subject.15 Pursuant to Article 24, second paragraph, of the GDPR, a

controller, where it is proportionate to the processing activities

about an appropriate data protection policy that is also implemented. These standards are evolving

elaborated in Chapter 2 of this report.

7 NEN 7510 (2017) Medical informatics – Information security in healthcare, part 2.

8 NEN 7513 (2018) Medical informatics - Logging - Recording actions on electronic patient files.

9 NEN 7510-2 (2017), section 9.4.1.

10 NEN 7510-2 (2017), section 9.1.1.

11 NEN 7510-2 (2017), section 12.4.1.

12 NEN 7513 (2018), sections 5.1, 6.2.1 and 6.2.2.

13 NEN 7510-2 (2017), section 12.4.1.

14 NEN 7510-2 (2017): section 7.2.1 and 7.2.2.

15 Explanatory Memorandum to the GDPR. Parliamentary Paper 34851, no. 3, p. 56-57.

2. Findings

2.1 Processing of personal data and the controller

2.1.1

2.1.2 Processing of patient data in the hospital information system

The subject of the AP's investigation is the processing of patient data in the hospital information system of the Haga Hospital.

The data relating to patients who enter the Haga Hospital in the hospital information system processes are personal data within the meaning of Article 4(1) of the GDPR16, because it contains information about identified17 natural persons. Some of this data is 'health data' the meaning of Article 9 of the AVG and can therefore be qualified as special personal data.

Furthermore, there is a processing of personal data within the meaning of Article 4, under 2 of the AVG.18 By its scope includes the concept of "processing" any possible operation or set of operations of personal data. This also includes consulting patient data in the hospital information system below.

Responsible

Since 2013, the Haga Hospital19 forms together with the Reinier de Graaf Gasthuis in Delft and (since 2015) the LangeLand Hospital in Zoetermeer the (foundation) Reinier Haga Group (RHG).20 Because of this partnership, the question must be answered which organization is the controller21 is responsible for the processing of patient data in the hospital information system of the Haga Hospital.

In this context, the AP considers that it has emerged that the management of the Haga Hospital independently manages the

institution

and management of the hospital information system. There is talk of an administrative merger and none

legal merger between the hospitals of the RHG and the hospitals within the RHG are system technical

16 Article 4, point 1 of the GDPR: ” “personal data” means any information relating to an identified or identifiable natural person

(“the data subject”); an identifiable natural person is one who can be identified, directly or indirectly,

in particular by means of an identifier such as a name, an identification number, location data, an online identifier or from

one or more elements characteristic of the physical, physiological, genetic, psychological, economic, cultural or social

identity of that natural person;”

17 Because, among other things, name and address details and also the BSN are processed, the identity of the persons is

established and it concerns

so identified persons.

18 Article 4(2) of the GDPR: ““processing” means any operation or set of operations relating to personal data or

a set of personal data, whether or not carried out by automated processes, such as collecting, recording, organizing,

structure, store, update or modify, retrieve, consult, use, provide by transmission, distribute

or otherwise making available, aligning or combining, blocking, erasing or destroying data;”.

19 The Haga Hospital Foundation is located in The Hague, Chamber of Commerce 27268552. Visiting address Els

Borst-Heilersplein 275, 2545AA The Hague.

20 https://www.hagaziekenhuis.nl/over-hagaziekenhuis/organisatie-en-bestuur.aspx.

21 Controller”: a natural or legal person, public authority, agency or other body

who, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4,

under 7, GDPR).

separated.22 The general RHG information security policy23 is fleshed out locally and the

Haga Hospital has its own authorization policy for digital patient files.24 In view of this, the AP is of

is of the opinion that the HagaZiekenhuis foundation is the controller within the meaning of Article 4, under 7, GDPR

for the processing of patient data in the hospital information system of the Haga Hospital.

The AP notes that the foundation could become RHG as co-controller

marked. The board of directors of the RHG foundation is responsible for the development and implementation

of hospital policy and the management and organization of hospital organisations.25 Nevertheless, the

management of the Haga Hospital has the most say over the local interpretation of the policy and thus

the Haga Hospital must be regarded as the (main) controller.

2.2 Authorizations (access control policy)

2.2.1 Elaboration of legal framework

Norm 9.1 of NEN 7510-2 (2017) stipulates that access to information must be limited. This serves

- inter alia - an access security policy must be established.26

Specifically for healthcare institutions, they must control access to health information. In the

in general, users of health information systems must control their access to personal

restrict health information to situations:

a) in which there is a care relationship between the user and the person to whom the data relates

have (the client whose personal health information is being accessed);

b) in which the user performs an activity on behalf of the person to whom the data relates;

c) where specific data is required to support this activity.

In addition, organizations that process personal health information must have an access control policy

(authorisations) with which access to this data is regulated. The policy of the

organization with regard to access control should be established on a prior basis

defined roles with associated privileges that match, but are limited to, the needs of

the roll.

The access control policy, as part of the information security policy framework, belongs

reflect professional, ethical, legal and client-related requirements and should perform duties

are performed by caregivers, and consider the workflow of the task.

The healthcare institution should have appropriate rules for access security, rights and restrictions for specific

establish user roles with respect to their assets, detailing and rigor of

the control measures reflect the related information security risks.

22 Statement of [CONFIDENTIAL] dated 31 October 2018 as stated in the report of official acts dated 19 December 2018, appendix 3, page 2. Also: https://www.hagaziekenhuis.nl/over-hagaziekenhuis/organisatie-en-bestuur.aspx.

23 Haga Hospital response dated October 23, 2018, Appendix 2: Reinier Haga Group Information Security Policy (version 1, December 2015).

24 Haga Hospital response dated October 23, 2018, Annex 3: Authorization of Digital Patient Files Haga Hospital (version 1.0, May 2018).

25 Reinier Haga Board Report 2017, p 33. https://www.reinierhaga.nl/jaarverslag/reinierhagagroep/2017/wp-content/uploads/2017/01/Board report-RHG-2017.pdf

26 Norm 9.1.1 of NEN 7510-2 (2017).

2.2.2

It is also important that, in order to prevent the provision of care from being delayed or halted, there should be more powerful ones

requirements then usually apply to a clear policy and process, with associated authorization, to ensure 'normal'

bypass access control rules in emergency situations.27

In concrete terms, with regard to a healthcare information system, the above means that the healthcare institution has roles must establish and apply with associated authorizations. Those authorizations should be 'appropriate'. That

means (the need for) access to health information and the limitations of access

depend on the role of the healthcare worker and the relationship with the patient (as evidenced by, for example,

treatment plan, work context, specialism, department, consultation), including the proper performance of the tasks that performed by healthcare providers into account.28

Factual findings

The AP notes that the Haga Hospital has an authorization policy based on

authorization profiles (roles/role-based access).29

The starting point of the authorization policy is that employees in the Haga Hospital have exclusive access
have access to patient data if they have a treatment agreement with the patient or if they
are directly involved in the implementation of a treatment agreement that a (other)
care provider within the organization has with the patient or act as a substitute for the other
healthcare provider (in summary, having a treatment relationship). An employee only needs access to this
access to the data necessary for his task in the context of the treatment agreement.
This not only concerns medical but also administrative support and management of the
institution, insofar as the data are necessary for this (for example, registering a patient, the
scheduling appointments, performing checks).30

According to the policy, the powers are limited to those patients with whom a
treatment relationship. The treatment relationship corresponds to the employee's work context.31 This also follows
from the authorization matrix sent by the hospital32 It follows from the authorization policy that
access to data must also be limited in time, namely for a period of one year, necessary to
to complete activities in the context of the treatment relationship.33

The AP notes that restrictions in access are concretely implemented because the authorizations of doctors,
physician assistants, nurses and other staff of support departments are based on it
specialism or the department for which they work or asked for a consultation with a specific patient

27 Norm 9.1.1 of NEN 7510-2 (2017).

28 See the AP's open letter to the boards of directors of healthcare institutions dated 15 February 2016;
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/open_brief_rvb_zorginstituut_15-02-2016.pdf.

29 Haga Hospital response dated October 23, 2018, Annex 3: Authorization of Digital Patient Files Haga Hospital (version 1.0,
May 2018).

30 Response HagaHospital dated October 23, 2018, Annex 3: Authorization Digital Patient Files HagaHospital (version 1.0,
May 2018),
page 3 and 4.

31 Response HagaHospital dated October 23, 2018, Annex 3: Authorization Digital Patient Files HagaHospital (version 1.0, May 2018), p 3 and 4.;

32 Response from Haga Hospital dated October 23, 2018, Appendix 6: Authorization Competence Matrix.

33 Reaction Haga Hospital dated October 23, 2018, Annex 3: Authorization Digital Patient Files Haga Hospital (version 1.0, May 2018), p 3.

are. Access to information from sensitive specialties (psychology, psychiatry, medical social work and sexology) is shielded hospital-wide. 34.35

In cases where the required availability of data for the care deviates from the set authorization, the hospital has a specific emergency button procedure (also known as “Breaking the glass” named). The screen shown contains a warning in which the user must specify the reason for access

36 The emergency button procedure is shown when:

- an employee visits a patient who is not known to the department/specialism for which there are rights are set. This means that it cannot be found in the outpatient clinic planning, work list or department occupancy list of the department(s)/speciality.
- an employee opens a file of a specialism for which he has no rights.37,38

The hospital also has a pseudonym procedure for shielding a patient at the hospital emergency room or an admitted patient when they need to be shielded for visits or family (for example, when there is abuse or removal of parental authority) or when the patient should not be found by searching by name via the 'search patient' functionality (e.g. known person or employee of the Haga Hospital).39

2.2.3 Assessment

In this study, the AP assesses the policy with regard to the granting of authorisations

(access control policy) and in general its application. The AP does not assess the individual authorizations40 of employees/roles.

The AP concludes that a context-bound method of authorization of employees has been provided, that the policy for setting authorizations has been carefully designed and that the correct starting points are used are used. The AP concludes on the basis of the statements of employees and the Haga Hospital provided documents that this policy is being implemented. That means it Haga Hospital's access control policy complies with standard 9.1.1 of the NEN 7510-2 (2017) and this means that appropriate measures are taken with regard to access control policy as required pursuant to Article 32 of the GDPR.

34 Response from Haga Hospital dated October 23, 2018, Appendix 6: Authorization Competence Matrix.

35 Statement of [CONFIDENTIAL] dated 31 October 2018 2018 as stated in the report of official acts dated 19 December 2018, Appendix 3, page 6.

36 Haga Hospital response dated October 23, 2018, Annex 3d of Annex 12: Communication expressions GDPR.

37 Response Haga Hospital dated October 23, 2018, Appendix 3: Authorization Digital Patient Files Haga Hospital (version 1.0, May 2018),

p. 4.

38 Hospital information system demonstration by [CONFIDENTIAL] dated October 31, 2018, as shown in the report of official acts dated December 19, 2018, appendix 3, page 3, 6-8.

39 Response from Haga Hospital dated October 23, 2018, Appendix 7: Procedure pseudonym.

40 The Haga Hospital found in mid-April 2018 that many authorizations were set too broadly and the authorization policy was revisited. This authorization policy is an ongoing process. (Statement of [CONFIDENTIAL] dated October 31, 2018 as reproduced in the report of official acts dated 19 December 2018, appendix 3, page 2; Haga Hospital response dated October 23

2018, Annex 14: Quick scan authorizations HiX.)

2.3 Authentication

2.3.1 Elaboration of legal framework

2.3.2

Standard 9.4. of the NEN 7510-2 (2017) stipulates that unauthorized access to systems and applications must be will be prevented. Health information systems that process personal health information41 this includes - among other things - establishing the identity of users and this should be done through authentication involving at least two factors42.43

This means that for access to patient data in the hospital information system of the Haga Hospital requires two-factor authentication. For example, authentication by means of something the user knows (a password or PIN) and something the user has (a token or smart card).

Factual findings

The AP notes that authentication of the identity of the employee in the Haga Hospital is at two ways is possible. Firstly, users can log in to the virtual workplace (VDI)44 through the staff pass for a card reader. Then the user enters his username, it password and a four-digit (user-specified fixed) PIN. There is a single-sign-on' functionality, which allows access to the VDI once logged in hospital information system.45 The user can then use the pass for four hours at any workstation log out and log in without entering a user name, password and/or pin code.46,47

Secondly, the user can log in to the VDI and the hospital information system without a staff pass with a user name and password, for example if the employee has forgotten the staff pass.48,49

2.3.3 Assessment

The strength of the user authentication should be appropriate for the classification of the information to which access is granted. In the hospital information system, data about health processed and requires two-factor authentication. Since users can access the data in the digital patient records with only something a user knows (namely a username

and password) in that case one factor is used. This does not fulfill it

41 NEN 7510-1 (2017), 3.44: “Information about an identifiable person related to the physical or mental condition of, or the provision of care services to, the person in question.”

42 In general, three factors are distinguished: something the user knows (a password or pin code); something that the user has (e.g. a token); or something the user is (a biometric). (Source: NCSC, Use two-factor authentication. Passwords all are not always sufficient. Factsheet FS-2015-02, version 1.1. October 22, 2018).

43 Norm 9.4.1 of NEN 7510-2 (2017).

44 Virtual Desktop Infrastructure.

45 Statement [CONFIDENTIAL] dated 31 October 2018 as stated in the report of official acts dated 19 December 2018, appendix 3, pages 3 , 7 and 8.

46 Virtual Workplace User Manual, version 6, publication date 8/14/2018, p. 2.

47 Demonstration hospital information system by [CONFIDENTIAL] dated October 31, 2018, as weather data in the report of official acts dated 19 December 2018, appendix 3, page 7.

48 Virtual Workplace User Manual, version 6, publication date 8/14/2018, p. 2.

49 Statement [CONFIDENTIAL] dated 31 October 2018 2018 as stated in the report of official acts dated 19 December 2018, Annex 3, pages 3, 7 and 8.

requirement of two-factor authentication. The Haga Hospital does not comply with standard 9.4.1 of the NEN on this point 7510-2 (2017) and therefore there are no appropriate measures with regard to authentication such as is required under Article 32(1) of the GDPR.

2.4 Logging

2.4.1 Elaboration of legal framework

Standard 12.4.1 of NEN 7510-2 (2017) stipulates, among other things, that log files should be made of events that include user activities, exceptions, and information security events register.50

In addition, it follows from standard 5.1 of the NEN 7513 (2018) that the logging must generally make it possible to determine irrefutably afterwards which events have taken place on a patient record. Among other things, the system must keep track of which event took place, the date and the time of the event, which client was involved and who the user was.

It is also important that all events involving actions that relate to a patient file (including viewing data) are logged;51 also events that do not fall under normal data access procedures, such as applying an emergency procedure (eg the “Breaking the glass” procedure).52

Factual findings

The Haga Hospital logs every access to digital patient files in the hospital information system, both access via the emergency button procedure and beyond. The logging shows which employee is on a has had access to the electronic patient file of the patient on a certain date and at a certain time patient.53,54,55

2.4.2

2.4.3 Assessment

The Haga Hospital logs all access to patient files and the log files offer the possibility to determine afterwards whether there has been abuse. With this, the Haga Hospital meets that requirement is indicated in NEN 7510 and 7513. This means that appropriate measures are taken with regard to logging as required under Article 32 of the GDPR.

50 The AP has not investigated the retention period of the log files.

51 NEN 7513 (2018) 6.2.1.

52 NEN 7513 (2018) 6.2.2.

53 Reaction Haga Hospital dated October 23, 2018, Annex 3: Authorization Digital Patient Files Haga Hospital (version 1.0, May 2018), p. 6.

54 Haga Hospital response dated October 23, 2018, Appendix 11: Logging.

55 Demonstration log file by [CONFIDENTIAL], on-site investigation dated October 31, 2018, as shown in the report of official acts dated December 19, 2018, appendix 3, page 3, 6-8.

2.5 Checking the Logging

2.5.1 Elaboration of legal framework

2.5.2

The requirements regarding registration and auditing are among the most important of all security requirements for protecting personal health information. These requirements guarantee accountability clients who entrust their information to electronic medical record systems and are also a strong incentive for the users of such systems to implement policies on it acceptable use of these systems. Effective auditing and registration can contribute to demonstrating misuse of health information systems or personal health information. These processes can also help organizations and clients obtain redress from users who abuse their access rights. Requirements for registering events are detailed in NEN 7513 discussed (explanation of standard 12.4.1 of NEN 7510-2 (2017)).
Norm 12.4.1 of NEN 7510-2 (2017) therefore stipulates that log files should be regularly rated. The AP applies the principle that there must be systematic, consistent control of all logging. A random check and/or a check based on complaints is not sufficient to fulfill this. The AP has these starting points in its report on security of digital patient records already described in 2013. It is also indicated that hospitals should strive for more 'intelligent' analysis or control of the logging.56 With these starting points, the AP is referring to the presence of a risk-oriented system for the checks, of which only random random checks and/or checks based on complaints of only a few files per year there is no question.

Factual findings

The policy for checking the logging of the Haga Hospital is, given the Authorization Policy and statements by Haga57,58 that periodically, i.e. once every two months, a check on the logging takes place by means of a random sample of 1 patient file. The authorization policy describes the intended checks on the logging: “A failed access attempt as well as a successful access to a digital file outside the treatment relationship, realized via the emergency button procedure, will be processed via this logging

56 See also report “Access to digital patient records within healthcare institutions” (2013), p. 13, 15-16 and 17. p. 13;” The Dutch DPA also notes that the health care institutions examined do not provide for systematic, consistent monitoring of all logging. At most, the logging is checked when the emergency button is used, which is – often – also limited to random checks or checks based on complaints. Healthcare institutions where there is no systematic control of all logging therefore do not comply with Article 13 of the Wbp.” (…) P.16:” The obligation to log to prevent unauthorized access as included in the NEN standards implies that the logging is actually checked. That control is one essential part of access security and is all the more important where in healthcare institutions the authorization – for the time being – falls short. If healthcare institutions improve those authorizations, the analysis of the logging may also be approached more 'intelligently' could be." (…) P.17: “In the health care institutions studied, there is no further provision for a systematic, consistent control of all logging. At most, the logging is checked when the emergency button is used, which is – often – also limited to random checks or checks based on complaints. The obligation to check the logging in order to check whether access to patient data is limited to situations where it is lawful, logically follows from the obligation to logging as included in NEN 7510 and NEN 7513. Healthcare institutions where no systematic check of all logging takes place, therefore do not comply with Article 13.” (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patient files within healthcare institutions.pdf)

57 Haga Hospital response dated October 23, 2018, answer to question 5 and Appendix 3: Authorization of Digital Patient Files

Haga Hospital (version 1.0, May 2018), p. 3 and 6.

58 Statement of [CONFIDENTIAL] dated 31 October 2018 dated 31 October 2018 as stated in the report of official acts dated 19 December 2018, appendix 3, pages 3-5.

regularly checked for legality. Such checks will be for regular patient records are performed on the basis of an audit. Checks for patient records belonging to treatment in the specialties of psychiatry, psychology, VIP, own staff and in relation to venereal diseases will be carried out in total.59

The AP has established that in the period from January to October 2018, a check of the logging has taken place with regard to the file of the patient referred to in paragraph 1.1 in accordance with the authorization policy.60,61 In view of the number of accesses to this specific file, further investigation has been launched into (un)lawful access.62

In addition, requests from patients and employees in six files were checked during that period unauthorized access occurred. No irregularities emerged from those checks come.63,64,65

There is no question of checking the logging of all files by selecting for striking deviations or outliers, nor is automatic signaling used when certain limits are exceeded limit values.66,67

The Haga Hospital has indicated that it intends to conduct six random samples do in 2019, in accordance with the policy. This includes access to the file of six different patients checked by various departments.68,69

2.5.3 Assessment

The policy for checking the logging of the Haga Hospital regulates that checking the legality of access to the patient files takes place via the logging of a random sample of six annually patient records, taking into account failed access attempts as well as actual access to the

digital file outside the treatment relationship, realized via the emergency button procedure. If selected

file belongs to one of the five 'sensitive' groups, the logging of that file must be complete

checked.

However, with a check of the logging of a random sample of six patient records annually,

the Haga Hospital does not have a policy with regard to systematic, risk-oriented or intelligent control of the

59 Haga Hospital response dated October 23, 2018, Annex 3: Authorization of Digital Patient Files Haga Hospital (version 1.0,

May 2018),

p. 3 and 6.

60 Response from Haga Hospital dated October 23, 2018, Appendix 1: Response to the AP regarding questions and research

announced October 31,

answer 5.

61 Statement of [CONFIDENTIAL] dated 31 October 2018 dated 31 October 2018 as stated in the report of official acts

dated 19 December 2018, appendix 3, pages 3-5.

62 View of the Haga Hospital on the provisional findings of the AP investigation, letter dated February 4, 2019.

63 Haga Hospital response dated October 23, 2018, Annex 1: Response to the AP regarding questions and research

announced October 31, 2018,

answer 5.

64 Statement of [CONFIDENTIAL] dated 31 October 2018 as stated in the report of official acts dated 19 December

2018, appendix 3, pages 4-5, and Haga Hospital response dated November 29, 2018 p. 1.

65 Haga Hospital response dated October 23, 2018, Appendix 11.

66 Haga Hospital Response dated October 23, 2018, Appendix 3: Authorization Digital Patient Files Haga Hospital (version

1.0, May 2018),

p. 6.

67 Statement [CONFIDENTIAL], 31 October 2018 as set out in the report of official acts dated 19 December 2018, appendix

3, pages 4-5.

68 Statement [CONFIDENTIAL], October 31, 2018 as set out in the report of official acts dated December 19, 2018,

appendix 3, page 4-5.

69 Haga Hospital response dated October 23, 2018, Appendix 19: Procedure Sample Logging and Planning Sample Logging.

logging. Also in practice no systematic check of the logging has taken place, because the inspections that did take place in the past period were in response to a number of complaints and requests but not risk-oriented and also insufficient in scope, given the scale of the processing of the hospital. This means that the Haga Hospital does not meet the standard 12.4.1 of the NEN 7510-2 (2017). This means that there are no appropriate measures with regard to checking the logging, such as is required under Article 32(1) of the GDPR.

With regard to the planned checks for 2019, the AP notes that a random sample check of six patient files per year is in any case not sufficient to meet the standard of systematic, risk-oriented or intelligent control.

2.6 Employee awareness

2.6.1 Elaboration of legal framework

The hospital should make employees aware of their responsibilities with regard to the information security. This includes appropriate awareness education and training for all employees receive and receive regular training in organizational policies and procedures, as relevant for the function. Employees should be made aware of disciplinary processes and consequences regarding information security violations. An awareness program should also be established established, with a number of activities, such as campaigns and the distribution of newsletters. This follows from standard 7.2.2 of NEN 7510-2 (2017).

Factual findings

The Haga Hospital provides information about information security as part of the introduction program for new employees, during work meetings and on the intranet. Furthermore, it has hospital participated in a national awareness campaign for employees aimed at the

importance of information security. In addition, AVG workshops have been held and all RHG

employees received a letter with an explanation as a result of the data breach in the second quarter of 2018

about the standard and possible sanctions.70,71,72

2.6.2

2.6.3 Assessment

In the opinion of the AP, the Haga Hospital has taken sufficient measures with regard to

the awareness of employees with regard to information security. With this it acts

Haga Hospital on this point in accordance with standard 7.2.2 of NEN 7510-2 (2017), which means that

of appropriate measures as required under Article 32 GDPR.

70 Haga Hospital response dated October 23, 2018, Appendix 12: Communication expressions GDPR.

71 Statements of [CONFIDENTIAL] dated October 31, 2018 as stated in the report of official acts dated December 19

2018, appendix 3, page 5 and response HagaHospital dated November 29, 2018 p. 1. and 2.

72 Statements of [CONFIDENTIAL], [CONFIDENTIAL] and [CONFIDENTIAL] dated October 31, 2018 as reflected in the

report

of official acts dated 19 December 2018, appendix 3, pages 9-11.

2.7 Conclusion on security aspects (article 32 GDPR)

The AP finds that the Haga Hospital has not taken sufficient appropriate measures in this regard

of the security aspects 'authentication' and 'checking the logging'. The Haga Hospital acts on this basis

contrary to article 32, first paragraph, opening words, of the GDPR.

With regard to the investigated security aspects 'authorisations', 'logging of access' and

'Awareness of employees with regard to information security', the AP finds no violations.

2.8 Reporting data breaches

2.8.1 Elaboration of legal framework

General

Articles 33 and 34 of the GDPR contain the 'obligation to report', which is known in common parlance data leaks', the obligation to report a personal data breach to the supervisory authority and the data subject.73

Data breach

The term 'data breach' does not appear in the law. Instead, the GDPR talks about a “related breach with personal data'.74 This is the case in the event of a security breach that occurs accidentally or on unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise processed.

Examples of data leaks are the loss of a USB stick with unencrypted personal data, a cyber attack in which personal data has been captured or an infection with ransomware in which personal data has been made inaccessible.

But unauthorized access to personal data is also a data breach. For example, in the case where employees of a hospital can view medical personal data of a patient75 without doing so competent, that is to say: without being directly involved in the treatment of the person in question patient and/or were involved in the administrative handling thereof.

Data breach notification obligation

In the event of a data breach (a breach), the controller is subject to two different reporting obligations:

(a) there is a reporting obligation to the AP (Article 33 GDPR); and

(b) there is an obligation to report to the data subject whose personal data it concerns (Article 34 GDPR).

A personal data breach must always be reported to the AP, unless it is not it is likely that the infringement poses a risk to the rights and freedoms of natural persons.” (Article 33, first paragraph, of the GDPR).

73 Explanatory Memorandum to the GDPR. Parliamentary Paper 34851, no. 3, p. 56-57.

74 Article 4(12) of the GDPR: . personal data breach” means a breach of security that is accidental or on unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or unauthorized access to transmitted, stored or otherwise processed data; “

75 Among other things, 'consulting' and 'requesting' personal data already constitutes 'processing' of personal data in the sense of the GDPR (Article 4 point 2 GDPR).

Furthermore, a personal data breach must be notified to the data subject if the it is likely that an infringement will result in a high risk to the rights and freedoms of natural persons persons (Article 34 paragraph 1 GDPR).

The threshold for communicating a breach to data subjects is therefore higher than the threshold for reporting a breach to the supervisory authority. Not all breaches need to be reported to data subjects reported, to prevent unnecessary notification fatigue.76 The controller must inform the assessment of the risk to the rights and freedoms of natural persons to take into account the specific circumstances of the infringement. In the 'Guidelines on the obligation to report data breaches'77, this assessment by the controllers.

However, even if it concerns data about health, not every unauthorized access by an employee of a healthcare institution leads to a probability of damage for the person concerned and thus to a high risk. Because not every unauthorized access is intentional or happens with wrong (unprofessional) intentions, such as curiosity. For example, if a wrong file is opened by mistake, or if it turns out afterwards that it was not necessary to view the data of a particular patient. In these cases is the patient still protected by the healthcare professional's professional ethics or support worker and it is not necessary - without further ado - to assume a 'probably (high) risk for the person concerned. However, it should always be determined by the specific circumstances of the case looked. These cases must be distinguished from the cases in which it does exist (intentionally) violating professional ethics. For example, if out of curiosity and without professional reason a medical file has been looked at (for example, in the file of a famous person, or of a family member or acquaintance.78) In such cases it is likely that the infringement will result in a high risk for the data subject and the breach must be reported to the AP and to the data subject.

Administration obligation data breaches

In addition, the controller is subject to an administrative obligation with regard to infringements

in connection with personal data. It follows from Article 33 paragraph 5 AVG that 'all infringements', therefore not

Notifiable breaches must be administered.

Written procedure for reporting data breaches

Pursuant to Article 24, paragraph 2, of the GDPR, a controller must submit this when

proportionate to the processing activities, to have an appropriate

data protection policy that is also implemented. That means that the Haga Hospital, because

many medical personal data79 are processed within it, as part of the

76 “Article 29” Working Group, Guidance on Personal Data Breach Notification under Regulation

2016/679, (Last revised and approved on February 6, 2018), (hereinafter: “Guidelines WP 29”), p. 23.

77 Guidance on personal data breach notification under Regulation 2016/679, revised on 6

February 2018, by WP29. (WP250rev.01)

(https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldmandatory_data leaks.pdf). These

"Guidelines

duty to report data leaks' of the consultative body of the European supervisors contain further explanation and guidelines for

the

notification of data breaches.

78 Although it may be assumed that the healthcare sector generally has a high level of professional ethics with regard to the

handling confidential and medical personal data, practice shows that this professional ethics is not always observed.

The case that gave rise to this investigation serves as an example.

79 The term used in the AVG and UAVG is: 'health data'; including Article 9, first paragraph, of the GDPR; that's a special one

category of (sensitive) personal data.

2.8.2

data protection policy must have a policy or a written procedure for

reporting data breaches and this policy must actually be implemented.

Factual findings

The AP notes that Haga Hospital has a specific written procedure for this

data leaks80 and the conversations held showed that the procedure is understood.81 This procedure

describes, in addition to a part of the standard explanation, the working method to be followed if an employee of the Haga Hospital

reports a possible data breach.

The procedure also mentions a number of examples of data leaks. There is a Commission

Data Breach, which consists of the Data Protection Officer and the Information Security Officer,

the executive secretary, the communications manager and the HR manager. If there is a large scale

data breach, the Commission can be expanded. The AP also notes that the Haga Hospital has an internal

has a register in which incidents are registered.82

2.8.3 Assessment

The AP concludes that the Haga Hospital has an internal data leak register and that the procedure

of the Haga Hospital with regard to registering and reporting data leaks, as described in the

document 'Procedure Notification Data Leak Haga Hospital' provides an appropriate interpretation of the obligations

of the Haga Hospital with regard to registering and reporting data leaks that follow from the articles

33 and 34 of the GDPR. Because the Haga Hospital has an appropriate written procedure

with regard to data breaches, Article 24(2) of the GDPR is complied with on this point83.

The AP notes that the "unauthorized access by its own employees to data about the health of

patients' is not mentioned as an example in the 'Procedure Notification Data Leak Haga Hospital' . The AP orders

Haga Hospital to supplement the document on this point.

80 HagaHospital Response dated October 23, 2018, Annex 5: Procedure for Reporting Data Breach HagaHospital, version 1.0; authorized on 18

October 2018.

81 Statement of [CONFIDENTIAL] dated 31 October 2018 2018 as stated in the report of official acts dated 19 December 2018, Appendix 3, page 5.

82 Response from Haga Hospital dated October 23, 2018, Annex 18: Register Data Leaks (version 1.0, May 2018).

83 The AP has not investigated the implementation or compliance with the procedure in concrete cases; so there is no mention of that stated in this report.

3. Conclusions

The AP has investigated whether the measures taken by the Haga Hospital in order to ensure that personal data in the digital patient file are not viewed by unauthorized employees, are appropriate as referred to in Article 32, paragraph 1, preamble, of the GDPR. The AP also has the policy of the Haga Hospital with regard to identifying and reporting data leaks examined (Articles 33 and 34 of the GDPR).

The AP finds that the Haga Hospital has not taken sufficient appropriate measures in this regard of the security aspects 'authentication' and 'checking the logging'. The Haga Hospital acts on this basis contrary to article 32, first paragraph, opening words, of the GDPR.

With regard to the security aspects examined, 'authorisations', 'logging of access', 'awareness employees with regard to information security', the AP finds no violations.

The AP also concludes that the Haga Hospital has an internal data leak register and that it written policy of the Haga Hospital with regard to registering and reporting data breaches is in accordance with Articles 33 and 34 of the GDPR and that Article 24, second member, of the AVG.

For this,

e.g.

3.1 Appendix 1: Response to Haga Hospital's opinion

In a letter with an appendix dated 16 January 2019, the AP sent the Haga Hospital a draft of the present research report, with the request to comment on it. The Haga Hospital made that one possibility of use by letter dated 4 February 2019. This appendix contains a response to this opinion.

General

Based on the opinion of the Haga Hospital, the draft research report has been revised points adjusted. It only concerns some textual changes.

The substantive view of the Haga Hospital pertains to two parts of the concept research report, namely 'checking the logging' and 'authentication'. Those topics are discussed below the order.

1. Checking the logging

View Haga Hospital:

The Haga Hospital notes in its opinion that the AP in its assessment in section 2.5.3 (Assessment control logging) states that the number of sample checks of six patient records is not sufficient to meet meet the standard of systematic control. The Haga Hospital has indicated in response that the NEN 7510 and 7513 do not speak of numbers, but of 'regular' checks. The Haga Hospital has asked the AP to indicate on the basis of which standard or policy it came to the conclusion that six samples would not be sufficient to meet the standard.

Reply AP:

The standard with regard to checking the logging has already been elaborated in section 2.5.1. It says in this described that inspections on the basis of NEN 7510 should take place 'regularly' and that the AP The starting point is that access control is systematic and consistent. A

random checks and/or a check based on complaints is not sufficient to give substance

to systematic and consistent access control. The AP has also described this starting point in the

previously published report 'Access to digital patient records within healthcare institutions' (2013), p 13, 15-16

and 17.84

View Haga Hospital:

The Haga Hospital has stated in its opinion that it explicitly strives for more intelligent analysis

of the logging and developments in this area. Soon the supplier will have a

giving the first presentation of such a recently completed module at the Haga Hospital.

Reply AP:

The AP takes note of the fact that the Haga Hospital expressly strives for 'more intelligent' analysis c.q.

checking the log. That does not alter the fact that the Haga Hospital does not yet meet the requirement

systematic consistent access control,

2. Authentication

View Haga Hospital:

The Haga Hospital indicates in its opinion that the DPA in its assessment of the authentication (section

2.3.3 Assessment) rightly states that this is insufficient and that in consultation with [CONFIDENTIAL] a short

the practical applicability of improvement measures on this point will be mapped out and

discussed in consultation with [CONFIDENTIAL].

Final Report 2019

20

Reply AP:

The AP takes note of the fact that the Haga Hospital acknowledges that it has fallen short on this point and that

improvement measures with regard to the authentication of users are mapped out. This takes

Nevertheless, the Haga Hospital has not yet sufficiently fulfilled the requirements imposed on the

user authentication.

84 https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-

healthcare institutions.pdf

Final Report 2019

21

Questions about the General Regulation

data protection

You will find information and answers to questions about the

General Data Protection Regulation (GDPR). Do you not have an answer to your question on this website?

found it? Then you can contact the Information and Reporting Center for Privacy of the Authority

Personal data on 088-1805 250.

About the Dutch Data Protection Authority

Everyone has the right to careful handling of their personal data. The Dutch Data Protection Authority supervises the

compliance with the legal rules for the protection of personal data and advises on new regulations.