Access to digital

patient records by

employees of the

HagaHospital

Research report

March 2019

Final report 2019

Index

Summary

When patients visit a hospital for treatment, they must be confident 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
have for the management settlement of the care or treatment, unauthorized in the
personal (medical) file. In case there is a leak of your personal
data, you as a patient want the hospital to report this to you and to the supervisor.
In October 2018, the Dutch Data Protection Authority (AP) investigated the measures taken by the
Haga Hospital has taken steps to ensure that personal data in the digital patient file is not
be viewed by unauthorized employees. In doing so, the AP has assessed whether these measures are 'appropriate'
are referred to in Article 32, first paragraph, preamble, of the General Data Protection Regulation (GDPR).
When assessing the security measures taken against Article 32 of the GDPR, the NEN 7510 and 7513 are as
measuring instrument used.
The AP also has the policy of the Haga Hospital with regard to identifying and reporting data leaks
investigated (Article 33 and 34 GDPR).
The AP has established that the Haga Hospital has not taken adequate measures with regard to
of the security aspects 'authentication' and 'control of the logging'. The Haga Hospital acts because of this
in violation of Article 32, first paragraph, preamble, of the GDPR.
With regard to the examined security aspects 'authorizations', 'logging of access' and
The AP does not find any violations for 'awareness of employees with regard to information security'.
The Haga Hospital has an internal data leak register; data leaks are registered there,
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 breaches is in accordance with
Articles 33 and 34 of the GDPR and that Article 24(2) of the GDPR is complied with in this regard.

1 Introduction

1.1 Background and aim of the study

The reason for the investigation is a report of a data breach from the Haga Hospital on April 4, 2018. The concerns a data breach in which it was established by HagaZiekenhuis that 85 of its employees have viewed data from a patient when he was admitted to the Haga Hospital, without doing so competent, i.e. without being directly involved in the handling of the concerned patient and/or were involved in the management settlement thereof. The patient was an acquaintance Dutchman. In mid-April 2018, various media reports appeared 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 HagaHospital. The investigation focuses on the situation in October 2018.

The main question in this research is the following:

Are the measures taken by the Haga Hospital to ensure that personal data the digital patient file cannot be viewed by unauthorized employees, 'appropriate' as referred to in Article 32 of the GDPR?

In this context, the AP has investigated the following aspects: authentication, authorizations, logging, control of logging and employee awareness.

The AP has also investigated the procedures for reporting data breaches (Article 33, first paragraph). paragraph, and Article 34, paragraph 1, of the GDPR).

1.2 Research progress

In a letter dated 12 October 2018, the AP initiated a further investigation and asked questions. The requested information was provided by the Haga Hospital in a letter dated 23 October 2018.

On October 31, 2018, four AP employees conducted an on-site investigation at the Haga Hospital, Leyweg location in The Hague, where the hospital information system was examined and

oral statements were also taken from [CONFIDENTIAL].

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

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

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

Haga Hospital responded in writing on February 4, 2019.

1 Following the report of the data breach, the AP asked the Haga Hospital on 23 April 2018 for information about 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 effect was applicable. As of May 25, 2018, the General Data Protection Regulation (GDPR) applies, as well as the GDPR Implementation Act (UAVG). The Wbp was also repealed on that date, pursuant to Article 51 of the UAVG.

The investigation by the AP at the Haga Hospital focuses on the situation in October 2018; that is, after the application of the GDPR.

Lawfulness of data processing

For employees of healthcare institutions, access to personal data about health in digitized patient records only lawfully if and insofar as an employee is directly involved in the treatment of or care to a patient and/or in the management of the management of that patient 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, pursuant to an office, profession or legal regulation or pursuant to a confidentiality agreement are required. This results 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 employee's fitness for work, medical diagnoses, the provision of health or social services or treatment or 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 the provisions of 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 they data are processed by or under the responsibility of a professional who, under Union or Member State law is bound by professional secrecy by law or by rules laid down by national competent authorities, or by another person who also under Union or Member State law or under rules adopted by national competent authorities secrecy has been kept.”

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

a.

care providers, institutions or facilities for health care or social services, to the extent that the processing is necessary for the proper treatment or care of the data subject or the management of the data concerning institution or professional practice;”

5 “If the first, second or third paragraph is applied, the data will only be processed by persons who are obliged to observe secrecy by virtue of an office, profession or legal regulation or by virtue of an agreement. If the controller processes personal data and not already on him by virtue of office, profession or law is subject to a duty of confidentiality, he is obliged to observe secrecy with regard to the data, except insofar as the law communication is required or the necessity arises from his task that the data be communicated to others who, pursuant to 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 inspection of or copies of the documents, referred to in Article 454, are provided then with

consent of the patient. If provision takes place, it will only take place insofar as this affects the personal privacy of another is not harmed. The provision may be made without taking into account 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 work to be performed by them in that context."

Security measures to be taken

Article 32, first paragraph, preamble, of the GDPR provides that the controller must provide appropriate technical and organizational measures to ensure a security level that is appropriate to the risk for the data subject guarantees. In doing so, the controller takes into account the available technology and the execution costs and with the nature, scope, context and purposes of the processing.

The 'Decree on electronic data processing by healthcare providers' includes further rules established on functional, technical and organizational measures for electronic data processing by healthcare providers. Pursuant to Article 3, second paragraph, and Article 5, first paragraph of the By decision, a healthcare provider must act in the security and logging of its healthcare information system in accordance with the provisions of NEN 7510 and NEN 7513.7.8 The standards NEN 7510 and NEN 7513 contain thus a mandatory further implementation of Article 32 of the GDPR 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 in the field of access to data in electronic patient records:

- Users are identified based on two-factor authentication.9

-

-

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

Log files are created to establish irrefutably afterwards which events

have taken place on a patient file.11,12

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

unlawful use of personal data.13

- Employees are made aware of their responsibilities in the area 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 breaches', the obligation to report a personal data breach to the

supervisory authority and the data subject.15 Pursuant to Article 24(2) of the GDPR, a

controller, when this is proportionate to the processing activities

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

detailed 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), paragraph 9.4.1.

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

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

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

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

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

15 MvT 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

processed, are personal data within the meaning of Article 4(1) of the GDPR16, as it contains information about

identified17 natural persons. Some of this data is 'health data' in

within the meaning of Article 9 of the GDPR and therefore qualify as special personal data.

Furthermore, there is a processing of personal data within the meaning of Article 4(2) of the GDPR.18 By

its scope, the term "processing" includes any possible operation or set of operations of

personal data. Consulting patient data in the hospital information system also falls there

below.

Responsible

Since 2013, the Haga Hospital19 has formed together with the Reinier de Graaf Gasthuis in Delft and (since 2015) the

LangeLand Hospital in Zoetermeer the (foundation) Reinier Haga Groep (RHG).20 Because of this

partnership, the question must be answered as to which organization

controller21 is for the processing of patient data in the

hospital information system of the Haga Hospital.

In this context, the AP considers that it has become apparent that the management of the Haga Hospital independently

and determines the management of the hospital information system. There is talk of an administrative merger and no

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

16Article 4(1) of the GDPR: “personal data” means any information relating to an identified or identifiable natural person (“the data subject”); considered identifiable is a natural person who can be identified, directly or indirectly, in particular by reference to 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 citizen service number are processed, the identity of the persons is established and concerns
so identified persons.

18 Article 4(2) of the GDPR: ““processing” means an operation or set of operations on personal data or a set of personal data, whether or not carried out via automated processes, such as collecting, recording, arranging, structure, store, update or modify, retrieve, consult, use, provide by forwarding, dissemination
or otherwise make available, align or combine, block, erase or destroy 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/about-hagaziekenhuis/organisation-en-bestuur.aspx.

21 Controller”: a natural or legal person, a public authority, a service or other body
which, 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 further elaborated locally and the Haga Hospital has its own authorization policy for digital patient files.24 In view of this, the AP of believes that the HagaZiekenhuis foundation is the controller within the meaning of Article 4(7) of the GDPR for the processing of patient data in the hospital information system of the Haga Hospital.

The AP notes that the RHG foundation could become a co-controller as a co-controller designated. 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
The management of the Haga Hospital has the most say over the local implementation of the policy and thus
Haga Hospital must be regarded as the (main) controller.

2.2 Authorizations (access control policy)

2.2.1 Elaboration of the legal framework

Standard 9.1 of NEN 7510-2 (2017) stipulates that access to information must be limited. To this end
- inter alia – to establish an access security policy.26
Specifically for healthcare institutions, they must control access to health information. In the
In general, users of health information systems should limit their access to personal
limit health information to situations:
a) in which there is a relationship of care 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 needed to support this activity.
In addition, organizations that process personal health information should have an access control policy
(authorisations) that regulate access to this data. The policy of the
organization with regard to access control should be established on the basis of prior
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, should be
reflect professional, ethical, legal and client-related requirements and the duties that
performed by caregivers, and taking into account the workflow of the task.
The healthcare facility should have appropriate access security rules, □rights and □restrictions for specific
establish user roles over their assets, specifying the details and rigor of
the controls are a reflection of the related information security risks.

22 Statement of [CONFIDENTIAL] dated October 31, 2018 as reflected in the record of official acts dated December 19

2018, appendix 3, page 2. Also: https://www.hagaziekenhuis.nl/over-hagaziekenhuis/organisatie-en-bestuur.aspx.

23 Response Haga Hospital dated 23 October 2018, Appendix 2: Information security policy Reinier Haga Groep (version 1, December 2015).

24 Haga Hospital response dated October 23, 2018, Appendix 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/renierhagagroep/2017/wp-content/uploads/2017/01/Management Report-RHG-2017.pdf

26 Standard 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 stalled, more powerful requirements then usually apply to a clear policy and process, with associated authorization, to ensure 'normal' circumvent access control rules in emergency situations.27

In concrete terms, the above means with regard to a health care information system that the health care institution plays a role and associated authorizations must be established and applied. Those authorizations should be 'appropriate'. That means that (the need for) access to health information and the restrictions on access depend on the role of the healthcare worker and the relationship with the patient (as shown, for example, by treatment plan, work context, specialism, department, consultation), including the proper execution of the tasks that are performed by health care providers.28

Actual 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 only have access have access to patient data if they have a treatment agreement with the patient or if they are directly involved in the performance of a treatment agreement that involves a (other)

care provider within the organization has with the patient or act as a replacement for that other healthcare provider (in summary, having a treatment relationship). An employee must only have access to have access to the data necessary for his task in the context of the treatment agreement.

This concerns not only medical but also administrative support and management of the institution, insofar as the data is necessary for this (for example, registering a patient, scheduling appointments, performing checks).30

According to the policy, the powers are limited to those patients with whom a logically treatment relationship. The treatment relationship corresponds to the employee's work context.31 This also follows from the authorization matrix sent by the hospital32 Incidentally, it follows from the authorization policy that access to data should also be limited in time, i.e. for a period of one year, necessary to to complete work 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 support staff are based on the specialism or the department for which they work or it was requested in consultation with a certain patient

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

28 See the open letter from the AP to the boards of directors of healthcare institutions dated February 15, 2016; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/open_brief_rvb_zorgbedrijven_15-02-2016.pdf.

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

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

p 3 and 4.

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

p 3 and 4.;

32 Haga Hospital response dated 23 October 2018, Appendix 6: Authorization Powers Matrix.

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

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

In cases where the required data availability for healthcare differs 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 where the user must state the reason for access

36 The emergency button procedure is displayed 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)/specialism.
- an employee opens a file of a specialty for which one has no rights.37,38

The hospital also has a pseudonym procedure for shielding a patient on the emergency department or an in-patient when they need to be shielded from visiting or family (for example, when there is abuse or deprivation of parental authority) or when the patient cannot 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 authorizations (access control policy) and its application in a general sense. The AP does not assess the individual authorizations40 of employees/roles.

The AP concludes that a context-bound method of authorization of employees is provided, that it is policy for setting authorizations has been carefully designed and that the correct principles

are used. The AP establishes 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 on the point of access control policy complies with standard 9.1.1 of 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 Haga Hospital dated 23 October 2018, Appendix 6: Authorization Powers Matrix.

35 Statement of [CONFIDENTIAL] dated 31 October 2018 2018 as reflected in the report of official acts dated 19

December 2018, Appendix 3, page 6.

36 Response Haga Hospital dated 23 October 2018, Appendix 3d of Appendix 12: Communications statements AVG.

37 Haga Hospital response dated October 23, 2018, Appendix 3: Authorization of Digital Patient Files Haga Hospital (version

1.0, May 2018),

p. 4.

38 Demonstration Hospital Information System by [CONFIDENTIAL] dated October 31, 2018, as reflected in the report of

official acts of 19 December 2018, appendix 3, page 3, 6-8.

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

40 In mid-April 2018, the Haga Hospital established that many authorizations had been set too broadly and the authorization

policy was subsequently

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; Reaction Haga Hospital dated October

23

2018, Appendix 14: Quick scan authorizations HiX.)

2.3 Authentication

2.3.1 Elaboration of the legal framework

2.3.2

Standard 9.4. of 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 include - among other things - establishing the identity of users and this should be done through authentication involving at least two factors42.43

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

Actual findings

The AP has established that authentication of the identity of the employee in the Haga Hospital takes two ways is possible. Firstly, users can log in to the virtual workplace (VDI)44 by using the holding a staff card in front of a card reader. Then the user enters his username, the 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 to the VDI hospital information system.45 The user can then spend four hours at any workstation with the pass log out and log in without entering a username, password and/or pin code.46,47

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

2.3.3 Assessment

The strength of 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 using only something a user knows (namely a username and password) in that case one factor is used. This does not comply with the

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 concerned.”

42 In general, three factors are distinguished: something the user knows (a password or PIN); something that the user has (for example, a token); or something that the user is (a biometric metric). (Source: NCSC, Use two-factor authentication. All passwords are not always enough. Factsheet FS-2015-02, version 1.1. October 22, 2018).

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

44 Virtual Desktop Infrastructure.

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

46 User manual Virtual Workplace, version 6, publication date 14-08-2018, p. 2.

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

48 User manual Virtual Workplace, version 6, publication date 14-08-2018, p. 2.

49 Statement [CONFIDENTIAL] dated 31 October 2018 2018 as reflected in the report of official acts dated 19 December 2018, Appendix 3, page 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 required under Article 32(1) of the GDPR.

2.4 Logging

2.4.1 Elaboration of the legal framework

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

In addition, it follows from standard 5.1 of NEN 7513 (2018) that logging in general must make it possible to establish irrefutably afterwards which events have taken place on a patient record. The system must, among other things, keep track of which event has occurred, the date

and the time of the event, which client was involved and who the user was.

Furthermore, it is important that all events involving actions related to a

patient file (including viewing data) are logged;51 also events that are not covered

under normal data access procedures, such as applying an emergency procedure (such as

the “Breaking the glass” procedure).52

Actual 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 record of the

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:

to determine afterwards whether there has been abuse. With this, the Haga Hospital complies with what

is specified in the 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 Haga Hospital response dated October 23, 2018, Appendix 3: Authorization of Digital Patient Files Haga Hospital (version

1.0, May 2018),

p. 6.

54 Response HagaZiekenhuis dated 23 October 2018, Appendix 11: Logging.

55 Demonstration log file by [CONFIDENTIAL], site investigation dated October 31, 2018, as reflected in the report of

official acts of 19 December 2018, appendix 3, page 3, 6-8.

2.5 Checking the logging

2.5.1 Elaboration of the legal framework

2.5.2

Registration and auditing requirements are among the most important of all security requirements for protecting personal health information. These requirements guarantee accountability for clients who entrust their information to electronic medical record registration systems and are also a powerful incentive for the users of such systems to acceptable use of these systems. Effective auditing and registration can contribute to demonstrating misuse of health information systems or of personal health information. These processes can also help organizations and clients obtain compensation from users who abuse their access rights. Requirements for event registration 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 assessed. The AP uses 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 included these principles in its report on security of digital patient records in 2013. It is also indicated that hospitals should striving for 'more intelligent' analysis and/or control of the logging.56 With these principles, the AP refers to the presence of a risk-oriented system in the checks, of which the only random random checks and/or checks based on complaints of only a few files per year there is no question.

Actual findings

The policy for checking the logging of the Haga Hospital is, in view of the Authorization Policy and statements from 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 realized access to
a digital file outside the treatment relationship, realized via the emergency button procedure, will be stored via this logging

56 See also report “Access to digital patient files within healthcare institutions” (2013), p. 13, 15-16 and 17.
p. 13;” The Dutch DPA also notes that the examined care institutions do not provide for a systematic, consistent check of
all logs. At the most, there is control of the logging when using the emergency button, which – often – is 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 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 constitutes a
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: “The researched health care institutions does not provide for a systematic, consistent control of
all logs. At the most, there is control of the logging when using the emergency button, which – often – is 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 control 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 Response to HagaZiekenhuis dated 23 October 2018, answer to question 5 and Appendix 3: Authorization of Digital Patient
Records
Haga Hospital (version 1.0, May 2018), p. 3 and 6.

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

are regularly checked for legality. Such checks will be carried out for regular

patient records are carried out 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 fact, 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 inspections in this specific file, further investigation has been initiated into

(un)lawful access.62

In addition, during that period, requests from patients and employees were subject to checks in six files

unauthorized access. No irregularities have emerged from these 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

limits.66.67

The Haga Hospital has indicated that it intends to take six random samples

do in 2019, in accordance with the policy. In addition, access to the file of six different patients is

from different 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 patient records is through the logging of a random sample of six . yearly

patient records, taking into account failed access attempts as well as realized access to the

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

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

checked.

However, checking 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, Appendix 3: Authorization of Digital Patient Files Haga Hospital (version 1.0, May 2018),

p. 3 and 6.

60 Response to Haga Hospital dated October 23, 2018, Appendix 1: Response to the AP regarding questions and announced research October 31,

answer 5.

61 Declaration of [CONFIDENTIAL] dated 31 October 2018 dated 31 October 2018 as reflected in the report of official acts dated 19 December 2018, appendix 3, page 3-5.

62 Haga Hospital's opinion on the preliminary findings of the AP investigation, letter dated 4 February 2019.

63 Response to Haga Hospital dated October 23, 2018, Appendix 1: Response to the AP regarding questions and announced research October 31, 2018,

answer 5.

64 Statement of [CONFIDENTIAL] dated October 31, 2018 as reflected in the record of official acts dated December 19 2018, appendix 3, page 4-5, and response HagaZiekenhuis dated 29 November 2018 p. 1.

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

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

p. 6.

67 Statement [CONFIDENTIAL], 31 October 2018 as reflected in the Report of Official Acts dated 19 December 2018, annex 3, page 4-5.

68 Statement [CONFIDENTIAL], 31 October 2018 as reflected in the Report of Official Acts dated 19 December 2018, Appendix 3, page 4-5.

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

log. In practice, too, no systematic control of the logging has taken place, because the checks that did take place in the past period were as a result of some complaints and requests but not risk-oriented and furthermore insufficient in size, given the scale of the processing of the hospital. This means that the Haga Hospital does not comply with the standard 12.4.1 of the NEN 7510-2 (2017). This means that there are no appropriate measures with regard to monitoring the logging such as 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 the legal framework

The hospital should make employees aware of their responsibilities regarding the information security. This includes all employees undergoing appropriate awareness education and training receive and regularly update organizational policies and procedures, as relevant for the function. Employees should be made aware of disciplinary processes and consequences with regarding information security violations. An awareness program should also be 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).

Actual findings

The Haga Hospital provides information about information security as part of the induction program for new employees, in work meetings and on the intranet. Furthermore, it has hospital participated in a national employee awareness campaign focused on 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. It deals with this

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

of appropriate measures as required under Article 32 GDPR.

70 Response Haga Hospital dated 23 October 2018, Appendix 12: Communication expressions AVG.

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

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

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

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

2.7 Conclusion on security aspects (Article 32 GDPR)

The AP has established that the Haga Hospital has not taken adequate measures with regard to

of the security aspects 'authentication' and 'control of the logging'. The Haga Hospital acts because of this

in violation of Article 32, first paragraph, preamble, of the GDPR.

With regard to the examined security aspects 'authorizations', 'logging of access' and

The AP does not find any violations for 'awareness of employees with regard to information security'.

2.8 Reporting data breaches

2.8.1 Elaboration of the legal framework

General

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

data breaches', 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 refers to a “breach of connection”

with personal data'.74 This is the case in the event of a security breach that is accidentally or 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 breaches include the loss of a USB stick containing unencrypted personal data, a cyber attack in which personal data is stolen or a ransomware infection 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 hospital staff can view a patient's medical personal data75 without doing so competent, i.e. without being directly involved in the handling of the concerned patient and/or were involved in the management settlement thereof.

Data breach notification obligation

In the event of a data breach (a breach), the controller has to deal with two different reporting obligations:

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

(b) there is a duty to report to the data subject whose personal data is concerned (Article 34 GDPR).

A personal data breach must always be reported to the AP, 'unless it's not' it is probable that the infringement poses a risk to the rights and freedoms of natural persons." (Article 33(1) of the GDPR).

73 MvT 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 unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of, or the unauthorized access to data transmitted, stored or otherwise processed; "

75 For example, in the case of 'consulting' and 'requesting' personal data, there is already a 'processing' of personal data in the meaning of the GDPR (Article 4(2) of the GDPR).

Furthermore, a personal data breach must be notified to the data subject if it

an infringement is likely to result in a high risk to the rights and freedoms of natural

persons (Article 34 (1) GDPR).

The threshold for communicating a breach to data subjects is therefore higher than that for reporting a breach

a breach of the supervisory authority. Not all breaches need to be disclosed to data subjects

reported, in order to avoid unnecessary notification fatigue.76 The controller should

assessment of the risk to the rights and freedoms of natural persons taking into account the

specific circumstances of the infringement. In the 'Guidelines on the obligation to report data breaches'77, this

assessment by the controllers in more detail.

However, even if health data is involved, not every unauthorized access by an employee

of a healthcare institution leads to a probability of harm to the person concerned and thus to a high

risk. Because not every unauthorized access is intentional or is done 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 data from a particular patient. In these cases

is the patient still protected by the healthcare professional's professional ethics or

support employee and it is not necessary - without further ado - to assume a 'probably'

(high) risk' for the person concerned. However, it must always be determined according to the specific circumstances of the

case

looked. These cases must be distinguished from cases in which the

(intentional) violation of professional ethics. For example if out of curiosity and without professional

reason has been looked into a medical file (for example, in the file of a famous person, or of a

relative or acquaintance.78) In such cases, it is likely that the infringement will result in a high

risk for the data subject and the infringement must be reported to the AP and to the data subject.

Administration obligation data leaks

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

in connection with personal data. It follows from Article 33 paragraph 5 of the GDPR that 'all infringements', so also not

notifiable breaches must be recorded.

Written procedure for reporting data breaches

Pursuant to Article 24, second paragraph, of the GDPR, a controller must, where required

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 Working Group “Article 29”, Guidelines for the reporting of personal data breaches under Regulation

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

77 Guidelines for the reporting of personal data breaches under Regulation 2016/679, revised on 6

February 2018, by WP29. (WP250rev.01)

(https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_dataleks.pdf). These 'Guidelines'

obligation to report data breaches' 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 in the healthcare sector in general there is a high professional ethics with regard to the

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

An example is the case that prompted this investigation.

79 The term used in the GDPR and UAVG is: “data about health”; i.a. Article 9(1) of the GDPR; that's a special one

category of (sensitive) personal data.

2.8.2

data protection policy must have a policy or written procedure for

reporting data breaches and this policy must also be implemented in practice.

Actual findings

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

data leaks80 and the interviews have shown that the procedure is understood.81 This procedure

describes, in addition to a part of the standard explanation, the procedure 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 breaches. 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 is 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 breaches, 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 at its disposal, with regard to data leaks, Article 24, second paragraph, of the GDPR is complied with in this respect.

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 recommends the Haga Hospital to supplement the document on this point.

80 HagaZiekenhuis response dated 23 October 2018, Appendix 5: Procedure for Notification of a HagaZiekenhuis data breach, version 1.0; authorized at 18 October 2018.

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

82 Haga Hospital response dated 23 October 2018, Appendix 18: Data Breach Register (version 1.0, May 2018).

83 The AP has not investigated the implementation or compliance with the procedure in specific cases; so no stated in this report.

3. Conclusions

The AP has investigated the question of whether the measures taken by the Haga Hospital are
in order to ensure that personal data in the digital patient record is not viewed by
unauthorized employees, are appropriate as referred to in Article 32, first paragraph, preamble, of the GDPR.
The AP also has the policy of the Haga Hospital with regard to identifying and reporting data leaks
investigated (Articles 33 and 34 of the GDPR).
The AP has established that the Haga Hospital has not taken adequate measures with regard to
of the security aspects 'authentication' and 'control of the logging'. The Haga Hospital acts because of this
in violation of Article 32, first paragraph, preamble, of the GDPR.
With regard to the examined security aspects 'authorisations', 'logging of access', 'awareness'
employees with regard to information security," the AP found no violations.
The AP also concludes that the Haga Hospital has an internal data leak register and that it is
Haga Hospital's written policy regarding the registration and reporting of data breaches in
is in accordance with Articles 33 and 34 of the GDPR and that in this respect Article 24, second
member of the GDPR.
Authority for Personal Data
For this,
w.g.
mr. drs. G.N.J.A. Bukkems
Director Customer Contact and Control Investigation
Final report 2019

3.1 Appendix 1: Response to Haga Hospital's opinion

In a letter with an attachment dated January 16, 2019, the AP sent the Haga Hospital a draft of the present
research report, with a request to comment on it. The Haga Hospital made that

possibility of use in letter dated 4 February 2019. This appendix contains a response to this opinion.

General

In response to the Haga Hospital's view, the draft research report has been

points adjusted. It concerns only some textual adjustments.

The substantive view of the Haga Hospital focuses on two parts of the concept

research report, namely 'control of the logging' and 'authentication'. Those topics will come next

the order.

1. Checking the logging

Haga Hospital's view:

In its view, the Haga Hospital notes that the AP in its assessment in section 2.5.3 (Assessment

control logging) states that the number of random checks of six patient records is not sufficient to meet

meet the standard of systematic control. In response, the Haga Hospital has indicated that

the NEN 7510 and 7513 do not speak of numbers, but of 'regular' checks. The Haga Hospital has

requested the AP to indicate on the basis of which standard or policy it comes to the conclusion that six

samples would not be sufficient to meet the standard.

Response AP:

The standard with regard to the control of logging has already been elaborated in section 2.5.1. This states

described that checks on the basis of NEN 7510 must take place 'regularly' and that the AP

The basic principle is that access control is systematic and consistent. A

random checks and/or a check on the basis of complaints is not sufficient to give substance

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

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

and 17.84

Haga Hospital's view:

The Haga Hospital has stated in its view that it is expressly striving for more intelligent analysis

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

give the first presentation of such a recently delivered module at the Haga Hospital.

Response AP:

The AP takes note of the fact that the Haga Hospital is emphatically striving for 'more intelligent' analysis and/or analysis. checking the log. This does not alter the fact that the Haga Hospital does not yet meet the requirement of systematic consistent access control,

2. Authentication

Haga Hospital's view:

In its view, the Haga Hospital indicates that the AP in its assessment of the authentication (section 2.3.3 Assessment) rightly states that this is insufficient and that in consultation with [CONFIDENTIAL] in the short term in due course the practical applicability of improvement measures in this regard is mapped and discussed in consultation with [CONFIDENTIAL].

Response 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 user authentication are mapped out. This takes

This does not mean that the Haga Hospital has currently insufficiently fulfilled the requirements for the authentication of users.

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

Questions about the General Regulation data protection

On our website Autoriteit Persoonsgegevens.nl 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 Privacy Information and Reporting Center 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 legal rules for the protection of personal data and advise on new regulations.