AUTORITEIT
PERSOONSGEGEVENS

Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis

Onderzoeksrapport

maart 2019

Definitief rapport 2019
[VERTROUWELIJK]

Inhoudsopgave

Samenvatting

Als patiënten een ziekenhuis bezoeken voor een behandeling dan moeten zij erop kunnen vertrouwen dat er vertrouwelijk met hun persoonsgegevens wordt omgegaan en dat er maatregelen zijn genomen om te voorkomen dat medewerkers, die geen behandelrelatie hebben met de patiënt of die de gegevens niet nodig hebben voor de beheersmatige afwikkeling van de zorgverlening of behandeling, onbevoegd in het persoonlijke (medische) dossier kijken. In het geval er toch sprake is van het lekken van je persoonlijke gegevens, wil je als patiënt dat het ziekenhuis dat aan jou en aan de toezichthouder meldt.

De Autoriteit Persoonsgegevens (AP) heeft in oktober 2018 onderzoek gedaan naar de maatregelen die het HagaZiekenhuis heeft getroffen om te waarborgen dat persoonsgegevens in het digitale patiëntdossier niet worden ingezien door onbevoegde medewerkers. Daarbij heeft de AP getoetst of die maatregelen 'passend' zijn als bedoeld in artikel 32, eerste lid, aanhef, van de Algemene Verordening Gegevensbescherming (AVG).

Bij toetsing van de getroffen beveiligingsmaatregelen aan artikel 32 van de AVG zijn de NEN 7510 en 7513 als meetinstrument gebruikt.

Ook heeft de AP het beleid van het HagaZiekenhuis ten aanzien van het signaleren en melden van datalekken onderzocht (artikel 33 en 34 AVG).

De AP constateert dat het HagaZiekenhuis onvoldoende passende maatregelen heeft getroffen ten aanzien van de beveiligingsaspecten 'authenticatie' en 'controle van de logging'. Het HagaZiekenhuis handelt hierdoor in strijd met artikel 32 , eerste lid, aanhef, van de AVG.

Ten aanzien van de onderzochte beveiligingsaspecten 'autorisaties', 'logging van de toegang' en 'bewustwording medewerkers ten aanzien van informatiebeveiliging' constateert de AP geen overtredingen.

Het HagaZiekenhuis beschikt over een intern datalekkenregister; daarin worden datalekken geregistreerd, ook als melden aan de AP en aan betrokkenen niet nodig is. De AP concludeert dat het schriftelijke beleid van het HagaZiekenhuis ten aanzien van het registeren en melden van datalekken in overeenstemming is met artikel 33 en 34 van de AVG en dat op dit punt wordt voldaan aan artikel 24, tweede lid, van de AVG.

1. Inleiding

1.1 Aanleiding en doel van het onderzoek

Aanleiding voor het onderzoek is een melding van een datalek van het HagaZiekenhuis op 4 april 2018. Het betreft een datalek waarbij door HagaZiekenhuis is geconstateerd dat 85 van zijn medewerkers de medische gegevens van een patiënt hebben ingezien toen deze was opgenomen in het HagaZiekenhuis, zonder daartoe bevoegd te zijn, dat wil zeggen: zonder dat zij direct betrokken waren bij de behandeling van de betreffende patiënt en/of betrokken waren bij de beheersmatige afwikkeling daarvan. De patiënt was een bekende Nederlander. Medio april 2018 zijn hierover in de media verschillende berichten verschenen.

Het ziekenhuis heeft na vragen van de Autoriteit Persoonsgegevens (AP) maatregelen aangekondigd.[1] Dit rapport bevat de uitkomsten van het nader onderzoek naar de beveiligingsmaatregelen van het HagaZiekenhuis. Het onderzoek is gericht op de situatie in oktober 2018.

De hoofdvraag in dit onderzoek is de volgende:
Zijn de maatregelen die het HagaZiekenhuis heeft getroffen, teneinde te waarborgen dat persoonsgegevens in het digitale patiëntdossier niet worden ingezien door onbevoegde medewerkers, 'passend' als bedoeld in artikel 32 van de AVG?

De AP heeft in dit kader de volgende aspecten onderzocht: authenticatie, autorisaties, de logging, de controle van de logging en de bewustwording van medewerkers.

Voorts heeft de AP onderzoek gedaan naar de procedures rond het melden van datalekken (artikel 33, eerste lid, en artikel 34, eerste lid, van de AVG).

1.2 Verloop onderzoek

Bij brief van 12 oktober 2018 heeft de AP een nader onderzoek ingesteld en vragen gesteld. De gevraagde informatie is bij brief van 23 oktober 2018 door het HagaZiekenhuis verstrekt.

Op 31 oktober 2018 hebben vier medewerkers van de AP een onderzoek ter plaatse uitgevoerd bij het HagaZiekenhuis, locatie Leyweg in Den Haag, waarbij het ziekenhuisinformatiesysteem is onderzocht en tevens mondelinge verklaringen zijn afgenomen van [VERTROUWELIJK].

Op 19 november 2018 heeft AP de verklaringen schriftelijk voorgelegd aan het HagaZiekenhuis. Het HagaZiekenhuis heeft hierop schriftelijk gereageerd 29 november 2018.

Op 16 januari 2019 heeft de AP de voorlopige bevindingen aan het HagaZiekenhuis toegestuurd. Het HagaZiekenhuis heeft schriftelijk gereageerd op 4 februari 2019.

[1] Naar aanleiding van de melding van het datalek heeft de AP op 23 april 2018 het HagaZiekenhuis verzocht om inlichtingen omtrent het datalek en de genomen maatregelen. Deze informatie is bij brief van 25 mei 2018 aan de AP verstrekt.

1.3 Wettelijk kader

Het datalek vond plaats in januari 2018, toen de Wet bescherming persoonsgegevens (Wbp) nog van toepassing was. Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing, alsmede de Uitvoeringswet AVG (UAVG). Tevens is op die datum de Wbp ingetrokken, ingevolge artikel 51 van de UAVG.

Het onderzoek van de AP bij het HagaZiekenhuis is gericht op de situatie in oktober 2018; dat wil zeggen ná het van toepassing worden van de AVG.

Rechtmatigheid gegevensverwerking
Voor medewerkers van zorginstellingen is toegang tot persoonsgegevens over gezondheid in gedigitaliseerde patiëntdossiers alleen rechtmatig indien en voor zover een medewerker rechtstreeks betrokken is bij de behandeling van of zorgverlening aan een patiënt en/of bij de beheersmatige afwikkeling van die behandeling/zorgverlening en de toegang beperkt blijft tot de gegevens die noodzakelijk zijn voor de uitvoering van de taken van die medewerker. Overigens geldt dat de persoonsgegevens alleen mogen worden verwerkt door personen die krachtens ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Dit vloeit voort uit het bepaalde in artikel 9 van de AVG, lid 2 onder h[2] en lid 3[3], artikel 30 van de UAVG, lid 3 onder a[4] en lid 4[5], en artikel 7:457 eerste en tweede lid Burgerlijk Wetboek (BW).[6]

[2] "de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;"

[3] "De in lid 1 bedoelde persoonsgegevens mogen worden verwerkt voor de in lid 2, punt h), genoemde doeleinden wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden."

[4] "Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door:

a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk;"

[5] "Indien toepassing wordt gegeven aan het eerste, tweede of derde lid, worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verwerkingsverantwoordelijke persoonlijk gegevens verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste, tweede of derde lid bevoegd zijn tot verwerking daarvan."

[6] "1. Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.
2. Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden."

Te treffen beveiligingsmaatregelen
Artikel 32, eerste lid, aanhef, van de AVG bepaalt dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treft om een op het risico voor betrokkene afgestemd beveiligingsniveau te waarborgen. Hierbij houdt de verwerkingsverantwoordelijke rekening met de beschikbare technologie en de uitvoeringskosten en met de aard, omvang, context en doeleinden van de verwerking.

In het 'Besluit elektronische gegevensverwerking door zorgaanbieders' zijn onder meer nadere regels vastgesteld over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door zorgaanbieders. Op grond van artikel 3, tweede lid, en artikel 5, eerste lid van het Besluit dient een zorgaanbieder bij de beveiliging en de logging van zijn zorginformatiesysteem te handelen overeenkomstig het bepaalde in NEN 7510 en NEN 7513.[7,8] De normen NEN 7510 en NEN 7513 bevatten daarmee een verplichte nadere invulling van artikel 32 van de AVG ten aanzien van een veilig en zorgvuldig gebruik van het zorginformatiesysteem van de zorgaanbieder. Daarom gebruikt de AP het bepaalde in NEN 7510 en NEN 7513 als norm bij de toetsing van door artikel 32 voorgeschreven 'passende technische en organisatorische maatregelen'.

De volgende eisen uit de NEN 7510 en NEN 7513 zijn betrokken bij de beoordeling van het passend niveau van de maatregelen die het ziekenhuis heeft getroffen op het gebied van toegangsverlening tot gegevens in elektronische patiëntdossiers:

- De identiteit van gebruikers wordt vastgesteld op basis van tweefactorauthenticatie.[9]
- Er is een toegangscontrolebeleid voor het verlenen van toegang tot informatie.[10]
- Er worden logbestanden gemaakt om achteraf onweerlegbaar vast te stellen welke gebeurtenissen hebben plaatsgevonden op een patiëntdossier.[11,12]
- De logbestanden worden regelmatig gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van persoonsgegevens.[13]
- Medewerkers worden bewust gemaakt van hun verantwoordelijkheden op het gebied van informatiebeveiliging.[14]

Deze normen worden verder uitgewerkt in Hoofdstuk 2 van dit rapport.

Melden van datalekken
De artikelen 33 en 34 van de AVG bevatten de in het normale spraakgebruik bekend staande 'meldplicht datalekken', de verplichting tot melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en de betrokkene.[15] Ingevolge artikel 24, tweede lid, van de AVG dient een verwerkingsverantwoordelijke, wanneer dat in verhouding staat tot de verwerkingsactiviteiten, te beschikken over een passend gegevensbeschermingsbeleid dat ook uitgevoerd wordt. Deze normen worden verder uitgewerkt in Hoofdstuk 2 van dit rapport.

[7] NEN 7510 (2017) Medische informatica – Informatiebeveiliging in de zorg, deel 2.
[8] NEN 7513 (2018) Medische informatica – Logging – Vastleggen van acties op elektronische patiëntdossiers.
[9] NEN 7510-2 (2017), paragraaf 9.4.1.
[10] NEN 7510-2 (2017), paragraaf 9.1.1.
[11] NEN 7510-2 (2017), paragraaf 12.4.1.
[12] NEN 7513 (2018), paragraaf 5.1, 6.2.1 en 6.2.2.
[13] NEN 7510-2 (2017), paragraaf 12.4.1.
[14] NEN 7510-2 (2017): paragraaf 7.2.1 en 7.2.2.
[15] MvT bij de AVG. Kamerstuk 34851, nr. 3, p. 56-57.

2. Bevindingen

2.1 Verwerking van persoonsgegevens en de verwerkingsverantwoordelijke

2.1.1 Verwerking van patiëntgegevens in het ziekenhuisinformatiesysteem

Onderwerp van het onderzoek van de AP is de verwerking van patiëntgegevens in het ziekenhuisinformatiesysteem van het HagaZiekenhuis.

De gegevens met betrekking tot patiënten die het HagaZiekenhuis in het ziekenhuisinformatiesysteem verwerkt, zijn *persoonsgegevens* in de zin van artikel 4, onder 1 van de AVG[16], omdat het informatie over geïdentificeerde[17] natuurlijke personen betreft. Een deel van deze gegevens zijn 'gegevens over gezondheid' in de zin van artikel 9 van de AVG en zijn derhalve te kwalificeren als bijzondere persoonsgegevens.

Voorts is sprake van een *verwerking* van persoonsgegevens in de zin van artikel 4, onder 2 van de AVG.[18] Door zijn reikwijdte omvat het begrip 'verwerking' elke mogelijke bewerking of geheel van bewerkingen van persoonsgegevens. Het raadplegen van patiëntgegevens in het ziekenhuisinformatiesysteem valt daar ook onder.

2.1.2 Verantwoordelijke

Sinds 2013 vormt het HagaZiekenhuis[19]samen met het Reinier de Graaf Gasthuis in Delft en (sinds 2015) het LangeLand Ziekenhuis in Zoetermeer de (stichting) Reinier Haga Groep (RHG).[20] Vanwege dit samenwerkingsverband moet de vraag worden beantwoord welke organisatie de verwerkingsverantwoordelijke[21] is voor de verwerking van patiëntgegevens in het ziekenhuisinformatiesysteem van het HagaZiekenhuis.

De AP overweegt in dit kader dat is gebleken dat de directie van het HagaZiekenhuis zelfstandig de inrichting en het beheer van het ziekenhuisinformatiesysteem bepaalt. Er is sprake van een bestuurlijke fusie en geen juridische fusie tussen de ziekenhuizen van de RHG en de ziekenhuizen binnen de RHG zijn systeemtechnisch

[16]Artikel 4, onder 1 van de AVG: " „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;"

[17] Omdat onder meer naam en adresgegevens en ook het BSN worden verwerkt, staat de identiteit van de personen vast en betreft het dus geïdentificeerde personen.

[18] Artikel 4, onder 2 van de AVG: "„verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;".

[19] Stichting HagaZiekenhuis is gevestigd te Den Haag, kvk 27268552. Bezoekadres Els Borst-Heilersplein 275, 2545AA Den Haag.

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

[21] Verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4, onder 7, AVG).

gescheiden.[22] Het algemene RHG informatiebeveiligingsbeleid[23] wordt lokaal nader ingevuld en het HagaZiekenhuis heeft een eigen autorisatiebeleid voor digitale patiëntdossiers.[24] Gelet hierop is de AP van oordeel dat de stichting HagaZiekenhuis verwerkingsverantwoordelijke is in de zin van artikel 4, onder 7, AVG voor de verwerking van patiëntgegevens in het ziekenhuisinformatiesysteem van het HagaZiekenhuis.

De AP merkt op dat de stichting RHG als mede-verwerkingsverantwoordelijke zou kunnen worden aangemerkt. De raad van bestuur van de stichting RHG is verantwoordelijk voor de ontwikkeling en uitvoering van het ziekenhuisbeleid en de sturing en inrichting van de ziekenhuisorganisaties.[25] Niettemin heeft de directie van het HagaZiekenhuis de meeste zeggenschap over de lokale invulling van het beleid en daarmee moet het HagaZiekenhuis als (hoofd-)verwerkingsverantwoordelijke worden aangemerkt.

2.2 Autorisaties (toegangscontrolebeleid)

2.2.1 Uitwerking juridisch kader

Norm 9.1 van de NEN 7510-2 (2017) bepaalt dat de toegang tot informatie moet worden beperkt. Hiertoe dient - onder meer – een beleid voor toegangsbeveiliging te worden vastgesteld.[26]

Specifiek voor zorginstellingen geldt dat zij de toegang tot gezondheidsinformatie moeten controleren. In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties:
a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt);
b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben;
c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen.

Voorts behoren organisaties die persoonlijke gezondheidsinformatie verwerken, een toegangscontrolebeleid (autorisaties) te hebben waarmee de toegang tot deze gegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole behoort te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot de behoeften van de rol.

Het toegangscontrolebeleid, als bestanddeel van het beleidskader voor informatiebeveiliging, behoort professionele, ethische, juridische en cliëntgerelateerde eisen te weerspiegelen en behoort de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking te nemen.

De zorginstelling behoort passende regels voor toegangsbeveiliging, -rechten en -beperkingen voor specifieke gebruikersrollen ten aanzien van hun bedrijfsmiddelen vast te stellen, waarbij de details en de striktheid van de beheersmaatregelen een afspiegeling zijn van de gerelateerde informatiebeveiligingsrisico's.

[22] Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 2. Ook: https://www.hagaziekenhuis.nl/over-hagaziekenhuis/organisatie-en-bestuur.aspx.
[23] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 2: Informatiebeveiligingsbeleid Reinier Haga Groep (versie 1, december 2015).
[24] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018).
[25] Reinier Haga Bestuursverslag 2017, p 33. https://www.reinierhaga.nl/jaarverslag/reinierhagagroep/2017/wp-content/uploads/2017/01/Bestuursverslag-RHG-2017.pdf
[26] Norm 9.1.1 van de NEN 7510-2 (2017).

Verder is belangrijk dat, om te voorkomen dat de verlening van zorg vertraagd wordt of stokt, er krachtigere eisen gelden dan gebruikelijk voor een duidelijk beleid en proces, met bijbehorende autorisatie, om 'normale' toegangscontroleregels in noodsituaties te omzeilen.[27]

Concreet betekent het bovenstaande ten aanzien van een zorginformatiesysteem dat de zorginstelling rollen met bijbehorende autorisaties moet vaststellen en toepassen. Die autorisaties behoren 'passend' te zijn. Dat betekent dat (de noodzaak voor) de toegang tot gezondheidsinformatie en de beperkingen van de toegang afhankelijk zijn van de rol van de zorgmedewerker en de relatie tot de patiënt (zoals blijkt uit bijvoorbeeld behandelplan, werkcontext, specialisme, afdeling, consultatie), daarbij de goede uitvoering van de taken die worden uitgevoerd door zorgverleners in aanmerking genomen.[28]

2.2.2 Feitelijke bevindingen

De AP constateert dat het HagaZiekenhuis beschikt over een autorisatiebeleid gebaseerd op autorisatieprofielen (rollen/role-based access).[29]

Uitgangspunt van het autorisatiebeleid is dat medewerkers in het HagaZiekenhuis uitsluitend toegang hebben tot patiëntgegevens indien zij een behandelingsovereenkomst hebben met de patiënt of als zij rechtstreeks betrokken zijn bij de uitvoering van een behandelingsovereenkomst die een (andere) zorgaanbieder binnen de organisatie heeft met de patiënt of optreden als vervanger van die andere zorgaanbieder (samengevat een *behandelrelatie* hebben). Daarbij dient een medewerker uitsluitend toegang te hebben tot de gegevens die noodzakelijk zijn voor zijn taak in het kader van de behandelingsovereenkomst. Het gaat daarbij niet alleen om medische maar ook om administratieve ondersteuning en beheer van de instelling, voor zover de gegevens daarvoor noodzakelijk zijn (bijvoorbeeld het inschrijven van een patiënt, het inplannen van afspraken, het uitvoeren van controles).[30]

De bevoegdheden zijn volgens het beleid ingeperkt tot die patiënten waarmee logischerwijs een behandelrelatie is. De behandelrelatie komt overeen met de werkcontext van de medewerker.[31] Dit volgt ook uit de autorisatiematrix die het ziekenhuis heeft toegestuurd[32] Overigens volgt uit het autorisatiebeleid dat toegang tot gegevens ook in tijd beperkt moet zijn, namelijk voor een periode van één jaar, noodzakelijk om werkzaamheden in het kader van de behandelrelatie af te ronden.[33]

De AP constateert dat beperkingen in toegang concreet worden ingevuld doordat de autorisaties van artsen, arts-assistenten, verpleegkundigen en overig personeel van ondersteunende afdelingen zijn gebaseerd op het specialisme c.q. de afdeling waarvoor zij werkzaam zijn of het bij een bepaalde patiënt in consult gevraagd

[27] Norm 9.1.1 van de NEN 7510-2 (2017).
[28] Zie de open brief van de AP aan de raden van bestuur van zorginstellingen van 15 februari 2016; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/open_brief_rvb_zorginstellingen_15-02-2016.pdf.
[29] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018).
[30] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p 3 en 4.
[31] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p 3 en 4.;
[32] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 6: Autorisatie Bevoegdhedenmatrix.
[33] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p 3.

zijn. Toegang tot informatie van gevoelige specialismen (psychologie, psychiatrie, medisch maatschappelijk werk en seksuologie) is ziekenhuisbreed afgeschermd. [34,35]

In gevallen waarin de vereiste beschikbaarheid van gegevens voor de zorg afwijkt van de ingestelde autorisatie beschikt het ziekenhuis over een specifieke noodknopprocedure (ook wel "Breaking the glass" genoemd). Het getoonde scherm bevat een waarschuwing waarbij de gebruiker de reden van inzage dient op te geven.[36] De noodknopprocedure wordt getoond wanneer:
- een medewerker een patiënt opzoekt die niet bekend is bij de afdeling/het specialisme waarvoor er rechten zijn ingesteld. Dit wil zeggen niet terug te vinden in de polikliniekplanning, werklijst of afdelingsbezettingslijst van de afdeling(en)/specialisme.
- een medewerker een dossier opent van een specialisme waar men geen rechten voor heeft.[37,38]

Verder beschikt het ziekenhuis over een schuilnaamprocedure voor afscherming van een patiënt op de spoedeisende hulp of een opgenomen patiënt wanneer deze moet worden afgeschermd voor bezoek of familie (bijvoorbeeld wanneer er sprake is van een mishandeling of ontzetting uit de ouderlijke macht) of wanneer de patiënt niet gevonden mag worden door het zoeken op naam via de 'patiënt zoeken' functionaliteit (bijv. bekend persoon of medewerker van het HagaZiekenhuis).[39]

2.2.3 Beoordeling

De AP beoordeelt in dit onderzoek het beleid ten aanzien van het toekennen van autorisaties (toegangscontrolebeleid) en in algemene zin de toepassing daarvan. De AP beoordeelt niet de afzonderlijke autorisaties[40] van medewerkers/rollen.

De AP concludeert dat is voorzien in een context-gebonden wijze van autorisatie van medewerkers, dat het beleid voor het instellen van autorisaties zorgvuldig is ingericht en dat daarbij de juiste uitgangspunten worden gehanteerd. De AP constateert op basis van de verklaringen van medewerkers en de door het HagaZiekenhuis verstrekte documenten dat dit beleid wordt uitgevoerd. Dat betekent dat het HagaZiekenhuis op het punt toegangscontrolebeleid voldoet aan norm 9.1.1 van de NEN 7510-2 (2017) en daarmee is sprake van passende maatregelen ten aanzien van toegangscontrolebeleid zoals vereist is ingevolge artikel 32 van de AVG.

[34] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 6: Autorisatie Bevoegdhedenmatrix.
[35] Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 6.
[36] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3d van Bijlage 12: Communicatie uitingen AVG.
[37] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p. 4.
[38] Demonstratie ziekenhuisinformatiesysteem door [VERTROUWELIJK] d.d. 31 oktober 2018, zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 3, 6-8.
[39] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 7: Procedure schuilnaam.
[40] Het HagaZiekenhuis constateerde medio april 2018 dat veel autorisaties te breed waren ingesteld en daarop het autorisatiebeleid opnieuw bekeken. Dit autorisatiebeleid is een doorlopend proces. (Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 2; Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 14: Quick scan autorisaties HiX.)

2.3 Authenticatie

2.3.1 Uitwerking juridisch kader

Norm 9.4. van de NEN 7510-2 (2017) bepaalt dat onbevoegde toegang tot systemen en toepassingen dient te worden voorkomen. Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie[41] verwerken behoren hiertoe - onder meer - de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren[42] worden betrokken.[43]
Dit betekent dat voor toegang tot patiëntgegevens in het ziekenhuisinformatiesysteem van het HagaZiekenhuis sprake dient te zijn van tweefactorauthenticatie. Bijvoorbeeld authenticatie door middel van iets dat de gebruiker weet (een wachtwoord of pincode) en iets dat de gebruiker heeft (een token of smartcard).

2.3.2 Feitelijke bevindingen

De AP constateert dat authenticatie van de identiteit van de medewerker in het HagaZiekenhuis op twee manieren mogelijk is. Ten eerste kunnen gebruikers inloggen op de virtuele werkplek (VDI)[44] door de personeelspas voor een paslezer te houden. Vervolgens voert de gebruiker zijn gebruikersnaam, het wachtwoord en een viercijferige (door de gebruiker opgegeven vaste) pincode in. Er is sprake van een 'single-sign-on' functionaliteit, waardoor eenmaal ingelogd op de VDI ook toegang mogelijk is tot het ziekenhuisinformatiesysteem.[45] De gebruiker kan daarna vier uren op een willekeurig werkstation met de pas af- en aanmelden zonder invoer van gebruikersnaam, wachtwoord en/of pincode.[46,47]

Ten tweede kan de gebruiker zonder personeelspas inloggen op de VDI en het ziekenhuisinformatiesysteem met een gebruikersnaam en wachtwoord, bijvoorbeeld als de medewerker de personeelspas is vergeten.[48,49]

2.3.3 Beoordeling

De sterkte van de gebruikersauthenticatie behoort passend te zijn voor de classificatie van de informatie waartoe toegang wordt verleend. In het ziekenhuisinformatiesysteem worden gegevens over gezondheid verwerkt en hiervoor is tweefactorauthenticatie vereist. Aangezien gebruikers toegang kunnen krijgen tot de gegevens in de digitale patiëntdossiers met alleen iets wat een gebruiker weet (namelijk een gebruikersnaam en wachtwoord) wordt in dat geval gebruik gemaakt van één factor. Daarmee wordt niet voldaan aan het

[41] NEN 7510-1 (2017), 3.44: "Informatie over een identificeerbare persoon die verband houdt met de lichamelijke of geestelijke gesteldheid van, of de verlening van zorgdiensten aan, de persoon in kwestie."
[42] Over het algemeen worden drie factoren onderscheiden: iets dat de gebruiker weet (een wachtwoord of pincode); iets dat de gebruiker heeft (bijvoorbeeld een token); of iets dat de gebruiker is (een biometrisch gegeven). (Bron: NCSC, Gebruik tweefactor-authenticatie. Wachtwoorden allen zijn niet altijd voldoende. Factsheet FS-2015-02, versie 1.1. 22 oktober 2018).
[43] Norm 9.4.1 van de NEN 7510-2 (2017).
[44] Virtual Desktop Infrastructure.
[45] Verklaring [VERTROUWELIJK] d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 3 , 7 en 8.
[46] Gebruikershandleiding Virtuele Werkplek, versie 6, publicatiedatum 14-08-2018, p. 2.
[47] Demonstratie ziekenhuisinformatiesysteem door [VERTROUWELIJK] d.d. 31 oktober 2018, zoals weergegevens in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 7.
[48] Gebruikershandleiding Virtuele Werkplek, versie 6, publicatiedatum 14-08-2018, p. 2.
[49] Verklaring [VERTROUWELIJK] d.d. 31 oktober 2018 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 3, 7 en 8.

vereiste van tweefactorauthenticatie. Het HagaZiekenhuis voldoet op dit punt niet aan norm 9.4.1 van de NEN 7510-2 (2017) en daarmee is geen sprake van passende maatregelen ten aanzien van authenticatie zoals vereist is ingevolge artikel 32, eerste lid, van de AVG.

2.4 Logging

2.4.1 Uitwerking juridisch kader

Norm 12.4.1 van de NEN 7510-2 (2017) bepaalt onder meer dat logbestanden behoren te worden gemaakt van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren.[50]

Daarnaast volgt uit norm 5.1 van de NEN 7513 (2018) dat de logging het in het algemeen mogelijk moet maken om achteraf onweerlegbaar vast te stellen welke gebeurtenissen hebben plaatsgevonden op een patiëntdossier. Het systeem moet onder meer bijhouden welke gebeurtenis heeft plaatsgevonden, de datum en het tijdstip van de gebeurtenis, welke cliënt het betrof en wie de gebruiker was.

Verder is het van belang dat *alle* gebeurtenissen waarbij acties plaatsvinden die betrekking hebben op een patiëntdossier (waaronder het inzien van gegevens) worden gelogd;[51] ook gebeurtenissen die niet vallen onder de normale procedures voor toegang tot gegevens, zoals het toepassen van een noodprocedure (zoals de "Breaking the glass" procedure).[52]

2.4.2 Feitelijke bevindingen

Het HagaZiekenhuis logt elke toegang tot digitale patiëntdossiers in het ziekenhuisinformatiesysteem, zowel de toegang via de noodknopprocedure als daarbuiten. Uit de logging blijkt welke medewerker op een bepaalde datum en bepaald tijdstip toegang heeft gehad tot het elektronisch patiëntdossier van de patiënt.[53,54,55]

2.4.3 Beoordeling

Het HagaZiekenhuis logt alle toegang tot patiëntdossiers en de logbestanden bieden de mogelijkheid om achteraf vast te stellen of sprake is geweest van misbruik. Hiermee voldoet het HagaZiekenhuis aan hetgeen hierover in de NEN 7510 en 7513 is aangegeven. Daarmee is sprake van passende maatregelen ten aanzien van logging zoals vereist is ingevolge artikel 32 van de AVG.

[50] De AP heeft geen onderzoek gedaan naar de bewaartermijn van de logbestanden.
[51] NEN 7513 (2018) 6.2.1.
[52] NEN 7513 (2018) 6.2.2.
[53] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p. 6.
[54] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 11: Logging.
[55] Demonstratie logbestand door [VERTROUWELIJK], onderzoek ter plaatse d.d. 31 oktober 2018, zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 3, 6-8.

2.5 Controle van de logging

2.5.1 Uitwerking juridisch kader

De eisen met betrekking tot het registreren en auditen behoren tot de belangrijkste van alle beveiligingseisen voor het beschermen van persoonlijke gezondheidsinformatie. Deze eisen garanderen rekenschap voor cliënten die hun informatie toevertrouwen aan elektronische registratiesystemen voor medische dossiers en zijn tevens een krachtige stimulans voor de gebruikers van dergelijke systemen om het beleid inzake het acceptabele gebruik van deze systemen na te leven. Doeltreffend auditen en registreren kan bijdragen aan het aantonen van misbruik van gezondheidsinformatiesystemen of van persoonlijke gezondheidsinformatie. Deze processen kunnen organisaties en cliënten ook helpen om schadeloosstelling te krijgen van gebruikers die hun toegangsrechten misbruiken. Eisen voor het registreren van gebeurtenissen worden in detail in NEN 7513 besproken (toelichting op norm 12.4.1 van de NEN 7510-2 (2017)).

Norm 12.4.1 van de NEN 7510-2 (2017) bepaalt dan ook dat logbestanden regelmatig behoren te worden beoordeeld. De AP hanteert hierbij als uitgangspunt dat sprake dient te zijn van systematische, consequente controle van alle logging. Een steekproefsgewijze controle en/of een controle op basis van klachten is niet voldoende om hier invulling aan te geven. De AP heeft deze uitgangspunten in haar rapport over beveiliging van digitale patiëntdossiers in 2013 reeds beschreven. Daarbij is ook aangegeven dat ziekenhuizen dienen te streven naar 'intelligentere' analyse c.q. controle van de logging.[56] Met deze uitgangspunten doelt de AP op het aanwezig zijn van een risicogerichte systematiek bij de controles, waarvan bij het enkel willekeurig steekproefsgewijs controleren en/of controleren op basis van klachten van slechts enkele dossiers per jaar geen sprake is.

2.5.2 Feitelijke bevindingen

Het beleid voor controle van de logging van het HagaZiekenhuis is, gezien het Autorisatiebeleid en verklaringen van Haga[57,58], dat periodiek, dat wil zeggen 1 keer in de twee maanden, een controle op de logging plaatsvindt door middel van een aselecte steekproef van 1 patiëntdossier. Het autorisatiebeleid beschrijft de voorgenomen controles op de logging:"*Een mislukte toegangspoging alsmede een gerealiseerde toegang tot een digitaal dossier buiten de behandelrelatie, gerealiseerd via de noodknopprocedure, zal via deze logging*

[56] Zie ook rapport " Toegang tot digitale patiëntendossiers binnen zorginstellingen" (2013), p. 13, 15-16 en 17.
p. 13;" Ook stelt het CBP vast dat in de onderzochte zorginstellingen niet is voorzien in een systematische, consequente controle van alle logging. Hoogstens is sprake van controle van de logging bij gebruik van de noodknop, hetgeen – veelal – ook beperkt blijft tot steekproefsgewijze controles of controle op basis van klachten. Zorginstellingen waar geen systematische controle van alle logging plaatsvindt, voldoen derhalve niet aan artikel 13 Wbp." (…) P.16:" De verplichting tot logging om onrechtmatige toegang te voorkomen zoals opgenomen in de NEN-normen impliceert dat de logging ook daadwerkelijk wordt gecontroleerd. Die controle vormt een wezenlijk onderdeel van de toegangsbeveiliging en is des te belangrijker daar waar in zorginstellingen de autorisatie – vooralsnog – tekortschiet. Als zorginstellingen die autorisaties verbeteren, zal de analyse van de logging mogelijkerwijs ook 'intelligenter' aangepakt kunnen worden." (…) P.17: "In de onderzochte zorginstellingen is verder niet voorzien in een systematische, consequente controle van alle logging. Hoogstens is sprake van controle van de logging bij gebruik van de noodknop, hetgeen – veelal – ook beperkt blijft tot steekproefsgewijze controles of controle op basis van klachten. De verplichting tot controle van de logging teneinde te controleren of toegang tot patiëntgegevens beperkt blijft tot situaties waarin dat rechtmatig is, vloeit logischerwijs voort uit de verplichting tot logging zoals opgenomen in NEN 7510 en NEN 7513. Zorginstellingen waar geen systematische controle van alle logging plaatsvindt, voldoen derhalve niet aan artikel 13." (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-zorginstellingen.pdf)
[57] Reactie HagaZiekenhuis d.d. 23 oktober 2018, antwoord op vraag 5 en Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p. 3 en 6.
[58] Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 3-5.

regulier worden gecontroleerd op rechtmatigheid. Dergelijke controles zullen voor reguliere patiëntendossiers op basis van een audit worden uitgevoerd. Controles voor patiëntendossiers behorende tot behandeling in de specialismen psychiatrie, psychologie, VIP, eigen personeel en in relatie tot geslachtsziektes zullen in totaliteit worden uitgevoerd.[59]

De AP stelt vast dat feitelijk in de periode vanaf januari tot en met oktober 2018 een controle van de logging heeft plaatsgevonden met betrekking tot het dossier van de in paragraaf 1.1 genoemde patiënt conform het autorisatiebeleid.[60,61] Gezien het aantal inzagen in dit specifieke dossier, is nader onderzoek ingesteld naar (on)rechtmatige inzage.[62]
Daarnaast hebben er in die periode op verzoeken van patiënten en medewerkers in zes dossiers controles op ongeautoriseerde inzage plaatsgevonden. Uit die controles zijn geen onregelmatigheden naar voren gekomen.[63,64,65]

Er is geen sprake van controle van logging van alle dossiers door te selecteren op opvallende afwijkingen of uitschieters, noch wordt gebruik gemaakt van automatische signalering bij overschrijding van bepaalde grenswaarden.[66,67]

Het HagaZiekenhuis heeft overigens aangegeven voornemens te zijn een zestal aselecte steekproeven te doen in 2019, conform het beleid. Daarbij wordt de toegang tot het dossier van zes verschillende patiënten van verschillende afdelingen gecontroleerd.[68,69]

2.5.3 Beoordeling

Het beleid voor controle van de logging van het HagaZiekenhuis regelt dat controle op de rechtmatigheid van toegang tot de patiëntdossiers plaatsvindt via de logging van een aselecte steekproef van jaarlijks zes patiëntdossiers, waarbij wordt gelet op mislukte toegangspogingen alsmede gerealiseerde toegang tot het digitaal dossier buiten de behandelrelatie, gerealiseerd via de noodknopprocedure. Indien een geselecteerd dossier hoort tot een van de vijf 'gevoelige' groepen, dient de logging van dat dossier volledig te worden gecontroleerd.

Echter, met een controle van de logging van een aselecte steekproef van jaarlijks zes patiëntdossiers, heeft het HagaZiekenhuis geen beleid ten aanzien van systematische, risicogerichte c.q. intelligente controle van de

[59] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p. 3 en 6.
[60] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 1: Reactie aan de AP inzake vragen en aangekondigd onderzoek 31 oktober as, antwoord 5.
[61] Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 3-5.
[62] Zienswijze HagaZiekenhuis op de voorlopige bevindingen van het AP onderzoek, brief d.d. 4 februari 2019.
[63] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 1: Reactie aan de AP inzake vragen en aangekondigd onderzoek 31 oktober 2018, antwoord 5.
[64] Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 4-5, en reactie HagaZiekenhuis d.d. 29 november 2018 p. 1.
[65] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 11.
[66] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 3: Autorisatie Digitale Patiënten Dossiers HagaZiekenhuis (versie 1.0, mei 2018), p. 6.
[67] Verklaring [VERTROUWELIJK], 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 4-5.
[68] Verklaring [VERTROUWELIJK], 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 4-5.
[69] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 19: Procedure Steekproef Logging en Planning Steekproef Logging.

logging. Ook in de praktijk heeft geen systematische controle van de logging plaatsgevonden, want de controles die de afgelopen periode wel hebben plaatsgevonden waren naar aanleiding van enkele klachten en verzoeken maar niet risicogericht en voorts in omvang onvoldoende, gelet op de schaal van de verwerking van het ziekenhuis. Dat betekent dat het HagaZiekenhuis niet voldoet aan de norm 12.4.1 van de NEN 7510-2 (2017). Daarmee is geen sprake van passende maatregelen ten aanzien van controle van de logging zoals vereist is ingevolge artikel 32, eerste lid, van de AVG.

Ten aanzien van de voorgenomen controles voor 2019 merkt de AP op dat een aselecte steekproefcontrole van zes patiëntendossiers per jaar in ieder geval niet voldoende is om aan de norm van systematische, risicogerichte c.q. intelligente controle te voldoen.

2.6 Bewustwording medewerkers

2.6.1 Uitwerking juridisch kader

Het ziekenhuis dient medewerkers bewust te maken van hun verantwoordelijkheden met betrekking tot de informatiebeveiliging. Hiertoe behoren alle medewerkers een passende bewustzijnsopleiding en –training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor de functie. Werknemers behoren te worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging. Ook dient een bewustzijnsprogramma te worden vastgesteld, met een aantal activiteiten, zoals campagnes en het verspreiden van nieuwsbrieven. Dit volgt uit norm 7.2.2 van NEN 7510-2 (2017).

2.6.2 Feitelijke bevindingen

Het HagaZiekenhuis verzorgt voorlichting over informatiebeveiliging als onderdeel van het introductieprogramma voor nieuwe medewerkers, in het werkoverleg en op intranet. Verder heeft het ziekenhuis deelgenomen aan een landelijke bewustwordingscampagne voor medewerkers gericht op het belang van informatiebeveiliging. Daarnaast zijn er AVG-workshops geweest en hebben alle RHG-medewerkers naar aanleiding van het datalek in het tweede kwartaal van 2018 een brief ontvangen met uitleg over de norm en mogelijke sancties.[70,71,72]

2.6.3 Beoordeling

Naar het oordeel van de AP heeft het HagaZiekenhuis voldoende maatregelen genomen, met betrekking tot de bewustwording van medewerkers ten aanzien van informatiebeveiliging. Hiermee handelt het HagaZiekenhuis op dit punt in overeenstemming met norm 7.2.2 van NEN 7510-2 (2017) en daarmee is sprake van passende maatregelen zoals is vereist ingevolge artikel 32 AVG.

[70] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 12: Communicatie uitingen AVG.
[71] Verklaringen van [VERTROUWELIJK] d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 5 en reactie HagaZiekenhuis d.d. 29 november 2018 p. 1. en 2.
[72] Verklaringen van [VERTROUWELIJK], [VERTROUWELIJK] en [VERTROUWELIJK] d.d. 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 9-11.

2.7 Conclusie beveiligingsaspecten (artikel 32 AVG)

De AP constateert dat het HagaZiekenhuis onvoldoende passende maatregelen heeft getroffen ten aanzien van de beveiligingsaspecten 'authenticatie' en 'controle van de logging'. Het HagaZiekenhuis handelt hierdoor in strijd met artikel 32, eerste lid, aanhef, van de AVG.

Ten aanzien van de onderzochte beveiligingsaspecten 'autorisaties', 'logging van de toegang' en 'bewustwording medewerkers ten aanzien van informatiebeveiliging' constateert de AP geen overtredingen.

2.8 Melden van datalekken

2.8.1 Uitwerking juridisch kader

Algemeen
De artikelen 33 en 34 van de AVG bevatten de in het normale spraakgebruik bekend staande 'meldplicht datalekken', de verplichting tot melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en de betrokkene.[73]

Datalek
De term 'datalek' komt niet voor in de wet. In de plaats daarvan heeft de AVG het over een 'inbreuk in verband met persoonsgegevens'.[74] Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Voorbeelden van datalekken zijn het verlies van een USB-stick met niet-versleutelde persoonsgegevens, een cyberaanval waarbij persoonsgegevens zijn buitgemaakt of een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Maar ook een onbevoegde inzage van persoonsgegevens is een datalek. Bijvoorbeeld in het geval waarbij medewerkers van een ziekenhuis medische persoonsgegevens van een patiënt inzien[75] zonder daartoe bevoegd te zijn, dat wil zeggen: zonder dat zij direct betrokken waren bij de behandeling van de betreffende patiënt en/of betrokken waren bij de beheersmatige afwikkeling daarvan.

Meldplicht datalekken
Bij een datalek (een inbreuk) heeft de verantwoordelijke te maken met twee verschillende meldplichten:
(a) er is een meldplicht aan de AP (artikel 33 AVG); en
(b) er is een meldplicht aan de betrokkene wiens persoonsgegevens het betreft (artikel 34 AVG).

Een inbreuk in verband met persoonsgegevens moet altijd gemeld worden aan de AP, '*tenzij het niet waarschijnlijk is* dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.' (artikel 33, eerste lid, van de AVG).

[73] MvT bij de AVG. Kamerstuk 34851, nr. 3, p. 56-57.
[74] Artikel 4, punt 12, van de AVG: . inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens; "
[75] Onder meer bij het 'raadplegen' en 'opvragen' van persoonsgegevens is reeds sprake van een 'verwerking' van persoonsgegevens in de zin van de AVG (artikel 4, punt 2, van de AVG).

Voorts moet een inbreuk in verband met persoonsgegevens worden gemeld aan de betrokkene als het *waarschijnlijk is* dat een inbreuk resulteert in *een hoog risico* voor de rechten en vrijheden van natuurlijke personen (artikel 34 lid 1 AVG).

De drempel voor het meedelen van een inbreuk aan betrokkenen ligt dus hoger dan die voor het melden van een inbreuk aan de toezichthoudende autoriteit. Niet alle inbreuken hoeven aan betrokkenen te worden gemeld, ter voorkoming van onnodige kennisgevingsmoeheid.[76] De verwerkingsverantwoordelijke dient bij de beoordeling van het risico voor de rechten en vrijheden van natuurlijke personen rekening te houden met de specifieke omstandigheden van de inbreuk. In de 'Richtsnoeren meldplicht datalekken'[77]wordt op deze beoordeling door de verwerkingsverantwoordelijken nader ingegaan.

Echter, ook al is sprake van gegevens over gezondheid, niet iedere onbevoegde inzage door een medewerker van een zorginstelling leidt tot een waarschijnlijkheid van schade voor de betrokkene en dus tot een hoog risico. Want niet iedere onbevoegde inzage is opzettelijk of gebeurt met verkeerde (onprofessionele) bedoelingen, zoals nieuwsgierigheid. Bijvoorbeeld, als per vergissing een verkeerd dossier wordt geopend, of als achteraf blijkt dat het niet nodig was om gegevens van een bepaalde patiënt in te zien. In deze gevallen wordt de patiënt nog steeds beschermd door de professionele beroepsethiek van de zorgverlener of ondersteunende medewerker en hoeft niet - zonder meer - te worden uitgegaan van een 'waarschijnlijk (hoog) risico' voor betrokkene. Wel moet altijd naar de specifieke omstandigheden van het geval worden gekeken. Deze gevallen moeten worden onderscheiden van de gevallen waarin wél sprake is van het (opzettelijk) schenden van de beroepsethiek. Bijvoorbeeld als uit nieuwsgierigheid en zonder professionele reden in een medisch dossier is gekeken (bijvoorbeeld in het dossier van een beroemd persoon, of van een familielid of kennis.[78]) In dergelijke gevallen is het wél waarschijnlijk dat de inbreuk resulteert in een hoog risico voor betrokkene en moet de inbreuk worden gemeld aan de AP én aan de betrokkene.

Administratieplicht datalekken
Daarnaast geldt er voor verwerkingsverantwoordelijke een administratieplicht met betrekking tot inbreuken in verband met persoonsgegevens. Uit artikel 33 lid 5 AVG volgt dat 'alle inbreuken', dus ook niet meldingsplichtige inbreuken, moeten worden geadministreerd.

Schriftelijke procedure voor het melden van datalekken
Ingevolge artikel 24, tweede lid, van de AVG dient een verwerkingsverantwoordelijke, wanneer dat in verhouding staat tot de verwerkingsactiviteiten, te beschikken over een passend gegevensbeschermingsbeleid dat ook uitgevoerd wordt. Dat betekent dat het HagaZiekenhuis, omdat daarbinnen veel medische persoonsgegevens[79] worden verwerkt, als onderdeel van het

[76] Werkgroep "Artikel 29", richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, (Laatstelijk herzien en goedgekeurd op 6 februari 2018), (hierna: 'Richtsnoeren WP 29'), p. 23.
[77] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, herzien op 6 februari 2018, door WP29. (WP250rev.01) (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf). Deze 'Guidelines meldplicht datalekken' van het overlegorgaan van de Europese toezichthouders bevatten nadere uitleg en richtsnoeren voor de melding van datalekken.
[78] Hoewel mag worden aangenomen dat in de zorgsector in het algemeen sprake is van een hoge beroepsethiek ten aanzien van de omgang met vertrouwelijke en medische persoonsgegevens, blijkt uit de praktijk dat deze beroepsethiek niet altijd wordt nageleefd. Als voorbeeld geldt de zaak die de aanleiding is van dit onderzoek.
[79] De in de AVG en UAVG gebruikte term is: 'gegevens over gezondheid'; o.a. artikel 9, eerste lid, van de AVG; dat is een bijzondere categorie van (gevoelige) persoonsgegevens.

gegevensbeschermingsbeleid dient over te beschikken over een beleid c.q. een schriftelijke procedure voor het melden van datalekken en dit beleid moet ook feitelijk uitgevoerd worden.

2.8.2 Feitelijke bevindingen

De AP constateert dat het HagaZiekenhuis beschikt over een specifieke schriftelijke procedure voor datalekken[80] en uit de gevoerde gesprekken is gebleken dat de procedure wordt begrepen.[81] Deze procedure beschrijft, naast een deel normuitleg, de te volgen werkwijze indien een medewerker van het HagaZiekenhuis een melding maakt van een mogelijk datalek.
In de procedure worden ook een aantal voorbeelden genoemd van datalekken. Er is een Commissie Datalekken, die bestaat uit de Functionaris voor de gegevensbescherming en de Information Security Officer, de directiesecretaris, de manager Communicatie en de HR-manager. Indien er sprake is van een grootschalig datalek, kan de Commissie worden uitgebreid. De AP constateert voorts dat het HagaZiekenhuis een intern register heeft waarin incidenten worden geregistreerd.[82]

2.8.3 Beoordeling

De AP concludeert dat het HagaZiekenhuis beschikt over een intern datalekkenregister en dat de procedure van het HagaZiekenhuis ten aanzien van het registeren en melden van datalekken, zoals beschreven in het document 'Procedure Melding Datalek HagaZiekenhuis' een passende invulling geeft van de verplichtingen van het HagaZiekenhuis ten aanzien van het registeren en melden van datalekken die volgen uit de artikelen 33 en 34 van de AVG. Doordat het HagaZiekenhuis beschikt over een passende schriftelijke procedure ten aanzien van datalekken, wordt op dit punt[83] voldaan aan artikel 24, tweede lid, van de AVG.

De AP merkt op dat de 'onbevoegde inzage door eigen medewerkers in gegevens over de gezondheid van patiënten' niet als voorbeeld wordt vermeld in de 'Procedure Melding Datalek HagaZiekenhuis' . De AP beveelt het HagaZiekenhuis aan om het document op dit punt aan te vullen.

[80] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 5: Procedure Melding Datalek HagaZiekenhuis, versie 1.0; geautoriseerd op 18 oktober 2018.
[81] Verklaring van [VERTROUWELIJK] d.d. 31 oktober 2018 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 5.
[82] Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 18: Register Datalekken (versie 1.0, mei 2018).
[83] De AP heeft geen onderzoek gedaan naar de uitvoering c.q. naleving van de procedure in concrete gevallen; daarover wordt dus geen uitspraak gedaan in dit rapport.

3. Conclusies

De AP heeft onderzoek verricht naar de vraag of de maatregelen die het HagaZiekenhuis heeft getroffen, teneinde te waarborgen dat persoonsgegevens in het digitale patiëntdossier niet worden ingezien door onbevoegde medewerkers, passend zijn als bedoeld in artikel 32, eerste lid, aanhef, van de AVG.

Ook heeft de AP het beleid van het HagaZiekenhuis ten aanzien van het signaleren en melden van datalekken onderzocht (artikel 33 en 34 van de AVG).

De AP constateert dat het HagaZiekenhuis onvoldoende passende maatregelen heeft getroffen ten aanzien van de beveiligingsaspecten 'authenticatie' en 'controle van de logging'. Het HagaZiekenhuis handelt hierdoor in strijd met artikel 32, eerste lid, aanhef, van de AVG.

Ten aanzien van de onderzochte beveiligingsaspecten 'autorisaties', 'logging van de toegang', 'bewustwording medewerkers ten aanzien van informatiebeveiliging' constateert de AP geen overtredingen.

Voorts concludeert de AP dat het HagaZiekenhuis beschikt over een intern datalekkenregister en dat het schriftelijke beleid van het HagaZiekenhuis ten aanzien van het registeren en melden van datalekken in overeenstemming is met artikel 33 en 34 van de AVG en dat op dit punt wordt voldaan aan artikel 24, tweede lid, van de AVG.

Autoriteit Persoonsgegevens
Voor deze,

w.g.

mr. drs. G.N.J.A. Bukkems
Directeur Klantcontact en Controlerend onderzoek

Bijlage 1: Reactie op zienswijze HagaZiekenhuis

Bij brief met bijlage van 16 januari 2019 zond de AP aan het HagaZiekenhuis een concept van het onderhavige onderzoeksrapport, met het verzoek daarop een zienswijze te geven. Het HagaZiekenhuis maakte van die mogelijkheid gebruik bij brief van 4 februari 2019. Deze bijlage bevat een reactie op deze zienswijze.

Algemeen
Naar aanleiding van de zienswijze van het HagaZiekenhuis is het concept-onderzoeksrapport op enkele punten aangepast. Het betreft uitsluitend enkele tekstuele aanpassingen.

De inhoudelijke zienswijze van het HagaZiekenhuis ziet op twee onderdelen van het concept-onderzoeksrapport, namelijk 'controle van de logging' en 'authenticatie'. Die onderwerpen komen hierna aan de orde.

1. Controle van de logging

Zienswijze HagaZiekenhuis:
Het HagaZiekenhuis merkt in haar zienswijze op dat de AP in haar beoordeling in paragraaf 2.5.3 (Beoordeling controle logging) stelt dat het aantal steekproefcontroles van zes patiëntendossiers nietvoldoende is om aan de norm van systematische controle te voldoen. Het HagaZiekenhuis heeft in reactie daarop aangegeven dat de NEN 7510 en 7513 niet spreken van aantallen, maar van 'regelmatige' controles. Het HagaZiekenhuis heeft de AP verzocht aan te geven op grond van welke norm of welk beleid zij tot de conclusie komt dat zes steekproeven niet voldoende zouden zijn om aan de norm te voldoen.

Reactie AP:
De norm ten aanzien van de controle van de logging is reeds uitgewerkt in paragraaf 2.5.1. Hierin staat beschreven dat controles op grond van de NEN 7510 'regelmatig' dienen plaats te vinden en dat de AP hierbij als uitgangspunt hanteert dat de controle van de toegang systematisch en consequent plaatsvindt. Een steekproefsgewijze controle en/of een controle op basis van klachten is niet voldoende om invulling te geven aan systematische en consequente toegangscontrole. De AP heeft dit uitgangspunt ook beschreven in het eerder verschenen rapport 'Toegang tot digitale patiëntendossiers binnen zorginstellingen' (2013), p 13, 15-16 en 17.[84]

Zienswijze HagaZiekenhuis:
Het HagaZiekenhuis heeft in haar zienswijze aangegeven uitdrukkelijk te streven naar intelligentere analyse van de logging en de ontwikkelingen op dit terrein nauwlettend te volgen. Binnenkort zal de leverancier een eerste presentatie van een dergelijke recent opgeleverde module bij het HagaZiekenhuis geven.

Reactie AP:
De AP neemt kennis van het feit dat het HagaZiekenhuis nadrukkelijk streeft naar 'intelligentere' analyse c.q. controle van de logging. Dat neemt niet weg dat het HagaZiekenhuis nu nog niet voldoet aan de eis van systematische consequente toegangscontrole,

2. Authenticatie

Zienswijze HagaZiekenhuis:
Het HagaZiekenhuis geeft in haar zienswijze aan dat de AP in haar beoordeling van de authenticatie (paragraaf 2.3.3 Beoordeling) terecht stelt dat dit onvoldoende is en dat in samenspraak met [VERTROUWELIJK] op korte termijn de praktische toepasbaarheid van verbetermaatregelen op dit punt in kaart worden gebracht en besproken in overleg met [VERTROUWELIJK].

Reactie AP:
De AP neemt kennis van het feit dat het HagaZiekenhuis erkent dat zij op dit punt tekort is geschoten en dat verbetermaatregelen ten aanzien van de authenticatie van gebruikers in kaart worden gebracht. Dit neemt niet weg dat het HagaZiekenhuis op dit moment onvoldoende invulling heeft gegeven aan de eisen die aan de authenticatie van gebruikers worden gesteld.

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

AUTORITEIT
PERSOONSGEGEVENS

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.