Zijn patiëntenzorg en privacy elkaars tegenpolen?

Met NEN7513 privacy en gegevensuitwisseling combineren

Mr. drs. J.A. van der Wel, Comfort-IA, jvdwel@comfort-ia.nl

25 februari 2020 met leesbaarheidsverbeteringen 20 januari 2021

Inleiding en samenvatting

Automatisering verbetert de toegankelijkheid van medische gegevens waardoor artsen hun patiënten beter kunnen behandelen. Het kabinet wil dan ook ruime toegang tot medische informatie voor spoedgevallen. Ook binnen de EU moeten patiëntgegevens worden uitgewisseld, stelde de Europese Commissie begin 2019[1]. Ruime dossiertoegang geeft echter nieuwsgierige medewerkers van zorginstellingen mogelijkheden om in dossiers te neuzen, zoals bleek uit mediaberichten over het OLVG in 2019 en het Haga ziekenhuis in 2018[2]. Het zeer kleine deel van de medewerkers dat tot dit gedrag geneigd is, is voldoende voor een negatief beeld. Toegankelijkheid van zorggegevens en privacy van de patiënt lijken zo elkaars tegenpolen.

Combineren van toegankelijkheid van gegevens en privacy is echter goed mogelijk en in dit artikel ga ik in op de mogelijkheden daarvoor. Twee elkaar aanvullende methodes komen aan de orde: afscherming van dossiers met behulp van account- en rechtenbeheer en achteraf verantwoording over inzagen met behulp van logging.

Afscherming met account- en rechtenbeheer verhindert onbevoegde inzagen en is daarom de betere aanpak. Helaas is die aanpak in de zorg lastiger in praktijk te brengen naarmate de schaal van gegevensuitwisseling groter wordt. Op regionaal en landelijk niveau zijn de pogingen met account- en rechtenbeheer tot nu toe niet van de grond gekomen.

Met achteraf verantwoorden is het kwaad al geschied als wordt geconstateerd dat onbevoegd is inzien maar logging van inzagen schrikt ook af omdat het de pakkans vergroot. Bij het weren van hackers in grootschalige systemen bestaat veel ervaring met logging van de gegevensinzage en het toezicht daarop. Voor zorginstellingen is logging een krachtig instrument voor toezicht op onbevoegde inzien door de eigen medewerkers.

Vanaf 2001 hebben patiënten recht op verantwoording achteraf van inzagen volgens de Wet bescherming persoonsgegevens (Wbp) [3] maar in de zorg heeft logging van gegevensinzage als privacy-instrument nog een flink potentieel aan niet gerealiseerde mogelijkheden. Een gestandaardiseerde manier waarop of zelfs een centrale plaats waar de patiënt de loggegevens kan bekijken, is wenselijk want dan hoeft de patiënt niet vertrouwd te raken met verschillende systemen van huisarts, apotheek, ziekenhuis en het uitwisselingssysteem daartussen et cetera. Een dergelijke oplossing vereist regie van de overheid om alle betrokken partijen op dezelfde lijn te krijgen, iets wat hierna buiten beschouwing blijft. Aan de orde komt wel dat logging standaarden of normen vereist. De norm “Vastleggen van acties op elektronische patiëntendossiers, NEN 7513”, hierna kortweg NEN 7513, geeft die al en ik ga in op de mogelijkheden om die norm aan te scherpen met ook aanbevelingen voor softwareleveranciers en zorginstellingen hoe beter gebruik te maken van die

norm en de daarmee samenhangende onderdelen uit de Norm voor Informatiebeveiliging in de Zorg, NEN 7510.

Account- en rechtenbeheer binnen zorginstellingen

De beste manier om gegevens af te schermen is toegangsmogelijkheden te laten samenvallen met de taken van medewerkers binnen de behandelteams. Daarvoor is beheer van accounts en toegangsrechten vereist maar dat kan lastig blijken.

Account- en rechtenbeheer vereist veel kennis en het is veel werk doordat dit op verschillende systemen nodig is. Vooral in de ziekenhuizen kan het aantal systemen oplopen, gemakkelijk tot rond de vijftien met daarnaast nog vele tientallen apparaten met losse meetgegevens van patiënten, zoals echo's of ECG's. Al die systemen en apparaten vereisen beheer van accounts en toegangsrechten van medewerkers die in dienst komen, van werkplek veranderen en weer uit dienst gaan. Soms kunnen rechten automatisch worden doorgegeven, vaak ook niet. Begrijpelijk is dan ook dat het College Bescherming Persoonsgegevens (CBP) in 2013 na onderzoek concludeerde dat de toegang tot digitale dossiers binnen zorginstellingen te ruim openstond[4].

Al met al is binnen een zorginstelling het rechtenbeheer goed mogelijk maar kan het kennisintensief, omvangrijk en foutgevoelig werk zijn.

Uitwisseling van gegevens tussen zorginstellingen: meer gegevens van patiënten en meer zorgmedewerkers

Na het verwerpen van het Landelijk EPD in 2011 werd het Landelijk Schakelpunt (LSP) in het leven geroepen met de Wbp als uitgangspunt. Patiënten doen mee na uitdrukkelijk toestemming. In 2016 werd deze mogelijkheid voor de zorg vastgelegd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)[5]. Vanaf medio 2020 moet de toestemming van de patiënt gespecificeerd kunnen worden voor categorieën van gegevens, categorieën van zorgaanbieders en individuele zorgaanbieders[6]. Uit de Memorie van Toelichting blijkt dat de minister wel wist dat dit lastig te realiseren was maar in 2016 verwachtte men nog dat dit met ICT ging lukken. Inmiddels is gebleken de patiënt er een lange lijst met vinkjes voor moeten bijhouden. Medewerkers binnen zorginstellingen met veel kennis van zaken kunnen dat maar voor de gemiddelde patiënt is dat ondoenlijk. De invoering van dit onderdeel is opgeschort en er wordt nu gezocht naar een andere mogelijkheid[7].

Verantwoording achteraf in het LSP blijkt wel te werken

Na de start van het LSP hebben de patiënten met de website https://www.volgjezorg.nl de mogelijkheid gekregen om te zien door wie, wanneer het dossier is geraadpleegd en wat daarbij is bekeken. Een rapport uit 2018[8] signaleert een forse groei van het aantal patiënten dat toestemming voor deelname gaf en groei van het aantal succesvolle gegevensraadplegingen. In dat rapport wordt de transparantie over wie de gegevens inziet, wanneer en wat wordt bekeken, cruciaal geacht voor het patiëntvertrouwen. Als verantwoording achteraf laagdrempelig mogelijk is op landelijke schaal, zou dat dan ook niet even laagdrempelig mogelijk moeten worden door zorginstellingen?

Verantwoording achteraf binnen de zorginstellingen, een recente historie

De wettelijke verplichting om de patiënt desgevraagd inzage te geven wie wanneer in zijn dossier heeft gekeken en wat daarbij werd gezien, werd voor zorginstellingen uitgewerkt in de Norm voor

informatiebeveiliging in de zorg in de versies van 2011 en 2017 met verwijzing naar NEN 7513[9]. Sinds begin 2018 verplicht het Besluit elektronische gegevensverwerking de toepassing van deze norm

Ondanks alle regels en normen bleek de invoering van NEN 7513, geen uitgemaakte zaak. In het eerdergenoemde onderzoek uit 2013 constateerde het CBP dat “de meeste onderzochte zorginstellingen niet structureel bijhouden wie wanneer welk patiëntendossier heeft geraadpleegd”. Ook de Nederlandse Vereniging van Ziekenhuizen merkte dit op bij de behandeling van de Wet Cliëntenrechtenzorg[10] en recent ook Liza van Lonkhuyzen en Jeroen Wester in de NRC naar aanleiding van patiëntervaringen[11]. Binnen de GGZ was één van de oorzaken dat enkele gangbare cliëntinformatiesystemen niet zonder ernstig performanceverlies konden loggen waardoor sommige instellingen zich gedwongen voelden om het log maar uit te zetten. Dat is tegenwoordig niet zonder risico want voor ontbrekend achteraf toezicht, is begin 2019 een forse boete opgelegd door de opvolger van het CBP, de Autoriteit Persoonsgegevens (AP)[12]. Het is de vraag of er geen betere aanpak is te bedenken om logging binnen zorginstellingen van de grond te laten komen dan handhaving door de AP met boetes.

Verantwoording achteraf binnen de zorginstellingen, de stand van zaken anno 2020

Met een klein informeel onderzoek onder informatiebeveiligers van zorginstellingen is de stand van zaken anno 2020 nagegaan en daarbij viel het volgende op.

- *Gebrek aan overzicht*

De centrale informatiesystemen in de zorg beschikken over een logmogelijkheid. Eén instelling verwacht van de leverancier op korte termijn noodzakelijke verbeteringen van de logging. Een CISO van een groot ziekenhuis merkte in dit verband op dat met logging in het centrale systeem een eerste stapje was gezet maar dat dat nog geen overzicht van alle dossierinzagen gaf omdat nog tal van andere systemen dossiergegevens bevatten zonder logging van inzagen. De problematiek verschilt per sector in de zorg want in een gesprek met een informatiebeveiliger uit de Jeugdzorg bleek de logging wel een goed overzicht te verschaffen.
Buiten beeld blijven ook nog de vragen die direct op de database worden uitgevoerd (“queries”), buiten het patiëntinformatiesystemen om. Zorginstellingen hebben deze mogelijkheid nodig om bijvoorbeeld statistieken te genereren of kostprijsberekeningen te kunnen maken en dergelijke maar langs deze weg kan ook patiëntinformatie worden opgevraagd.

Een overzicht van inzagen vereist ook dat de logs uit al die systemen worden gecombineerd in een verzamelbestand waaruit geautomatiseerd signalen kunnen worden gegenereerd, bijvoorbeeld van frequente gegevensinzagen van bekende Nederlanders. Ook handmatig onderzoek moet mogelijk zijn. Met deze aanpak bestaat veel ervaring bij het beheer van informatiesystemen om bijvoorbeeld hackersactiviteiten op te sporen. De aanpak staat bekend als Security Information and Event Management, SIEM en er is gespecialiseerde software voor verkrijgbaar in de markt.

NEN 7513 verwijst al naar de gestandaardiseerde bestandsindeling die nodig is voor het verzamelbestand en de Norm voor Informatiebeveiliging in de Zorg noemt een SIEM[13].

Een leverancier heeft nu een SIEM ontwikkeld voor de zorg en een aantal instellingen gaat de logging van uit verschillende modules die leverancier combineren.

- *Inbouwen van logging van inzagen is geen sinecure*

Inbouwen van logging van inzagen in een bestaand systeem blijkt om meerdere redenen lastig.

Allereerst ontstaan vragen bij het realiseren van het log. Een overzicht van patiënten, afdelingen en telefoonnummers is bijvoorbeeld handig voor de receptie om telefoonnummers op te zoeken. Die lijst is vertrouwelijk, zeker in een GGZ-instelling. Iedereen loggen die op die lijst voorkomt, ook als die toevallig op het scherm voorkomt bij de persoon waarnaar is gevraagd, leidt tot een zee aan loggegevens waarin het belangrijkste gegeven verdrinkt. Een oplossing is om de gegevens op het overzichtsscherm maar niet te loggen, een andere oplossing is de zoekmogelijkheid aanpassen om de overmaat aan logging te vermijden maar dat vereist extra werk voor ontwerp en realisatie en kan minder handig zijn om te gebruiken. NEN 7513 geeft geen houvast bij dit soort vragen.

Het kan ook lastig en kostbaar zijn om logging in te bouwen in oudere systemen die nog goed functioneren zoals een MRI- of labsysteem.

Tenslotte blijkt het realiseren van logging van inzagen specifieke programmeringsvaardigheden te vereisen[14] waarover leveranciers niet altijd beschikken. Naast het eerdergenoemde performanceverlies moet bijvoorbeeld ook rekening worden gehouden met de opslagkosten want logging van raadplegingen levert grote hoeveelheden gegevens per dag op. Daar komt bij dat recentelijk de bewaartermijn voor loggegevens is verlengd naar vijf jaar (ruim 1800 dagen)[15].

In de gesprekken die ik voerde, kwam een zorgsysteem naar voren dat de loggegevens weg zou schrijven naar de patiëntendatabase die de hele organisatie moet bedienen en daarom op duurdere, snelle opslagmedia staat met zware back-up en herstelprocedures. Met een kleine voorziening in de software zou een zorginstelling ervoor kunnen kiezen om de loggegevens weg te schrijven naar een apart, goedkoper medium want die gegevens worden niet vaak geraadpleegd en al helemaal niet gewijzigd.

- *Over prioriteiten denken leveranciers verschillend*

Bij de leveranciers vechten de prioriteiten soms om voorrang en logging kan het makkelijk verliezen van leuke dingen voor de gebruikers. Veel Nederlandse software wordt maar in een klein gespecialiseerd segment van de zorg gebruikt waardoor investeringen moeten worden terugverdiend over een kleine doelgroep en wijzigingen stap voor stap gaan.

Voor internationale leveranciers ligt dit anders. Die hebben een grote internationale markt waarin de Nederlandse markt klein is wat aparte regelingen onaantrekkelijk kan maken.

- *Wie doet er wat volgens NEN 7513?*

Bij inkoop van software verlangen zorginstellingen van leveranciers gewoonlijk dat zij aan allerlei NEN-normen te voldoen[16] waaronder NEN 7513. Leveranciers kunnen echter hooguit verantwoordelijk zijn voor een deel van zo'n norm, een ander deel moet de zorginstelling zelf uitvoeren[17]. Sommigen leveranciers vragen zich af hoe serieus zorginstellingen genomen moeten worden met deze vragen.

- *NEN 7513 wordt maar beperkt gebruikt*

Enkele leveranciers hebben recentelijk samengewerkt met een klant van hen om de logging te verbeteren. Daarbij is uitgegaan van al eerdere aanwezige logging en niet van de eisen en inrichtingsvoorschriften van NEN 7513. Een andere leverancier is bezig met de ontwikkeling van een SIEM voor de eigen software. Dat zou in principe ook signalen kunnen genereren uit de logs van software van andere leveranciers maar omdat de leverancier uitgaat van eigen coderingen, niet van die van NEN 7513, is dat pas te doen na vertaalslagen tussen die codes. Een zorginstelling kan die vertaalslagen best maken maar NEN 7513 bevat die codevoorschriften gebaseerd op internationale standaarden nu juist om die extra technische klus voor de IT-afdeling te vermijden omdat die toch al

de handen vol heeft aan het in bedrijf houden van de vele verschillende softwarepakketten en operating systems.[18]

Bij het inrichten van het SIEM lopen leveranciers en zorginstellingen nog tegen vragen op. Een voorbeeld is een signaal dat iemand in een ziekenhuis gegevens bekijkt van iemand die in dezelfde straat woont. Om dat signaal te genereren moet de patiëntendatabase worden geraadpleegd, is dat toegestaan? Daarbij komt het gedrag van een medewerker centraal te staan, is dat toegelaten lettend op de privacy van de medewerker of weegt toch het belang van patiënten het zwaarst? Verder kan het definiëren van automatisch te genereren signalen veel inventiviteit vereisen en het kan zinvol zijn om dat op één plaats uit te werken met ook aandacht voor controlefrequentie en -diepgang.

- *Voldoet de software aan NEN 7513?*

Voor een zorginstelling is het een hele klus om vast te stellen of software werkt volgens NEN 7513. Certificering van de software bespaart zorginstellingen dit werk.

Aanbevelingen voor betere logging

De conclusie is dat er interessante ontwikkelingen zijn op gebied van logging, maar dat er op een aantal punten verbeteringen mogelijk zijn met de volgende acties:

- *Door het Nederlands Normalisatie-instituut:*

NEN 7513 geeft al een heldere beschrijving van de logging van patiëntinformatiesystemen maar de praktijk houdt nog vragen.

Patiëntendossiers kunnen ook buiten het patiëntinformatiesysteem om worden opgevraagd met vragen direct op de patiëntendatabase of kopieën daarvan (“query’s”) en NEN 7513 zou hier ook op kunnen ingaan op de logging daarvan voor zover het opvraging van individuele patiënten betreft. Voor de overzichtschermen van de patiëntsystemen zijn aanbevelingen wenselijk om het aantal logsignalen te begrenzen dan wel maar te accepteren dat die buiten de logging worden gelaten.

NEN 7513 kan ook ingaan op het geautomatiseerd genereren van signalen. Wat mag wel en wat mag niet lettend op de privacy van medewerkers en combineren van het log en de patiëntendatabase. Ook richtlijnen voor controlefrequentie en -diepgang van controles kan een nuttige aanvulling zijn met wellicht ook een basislijst van geautomatiseerd te genereren signalen.

Verder nemen leveranciers NEN 7513 serieuzer als deze wordt gesplitst in een deel dat van toepassing is op de software en een deel dat de zorginstelling zelf moet realiseren. Dit zou kunnen met een technisch voorschrift op dezelfde manier waarop dit momenteel gebeurt voor beveiligde e-mail met de NTA 7516 als technische uitwerking en de NCS 7516 als certificeringsschema voor veilige email in de zorg. Dit opent de mogelijkheid van certificering die zorginstellingen werk kan besparen omdat dan de toets van voldoen aan de norm maar eenmalig hoeft te worden uitgevoerd door een certificerend bureau. Voor de logging door uitwisselingssystemen van de Wabvpz kan deze aanpak ook gelden, NEN 7513, is hierop al ingericht.

Tenslotte kan NEN 7513 ook aandacht schenken aan kwaliteitseisen die aan de software worden gesteld lettend op bijvoorbeeld performance en mogelijkheden om opslagkosten te beheersen.

- *Door de softwareleveranciers:*

De softwareleveranciers die dat nog niet hebben gedaan, zouden er goed aan doen om prioriteit te geven aan het voldoen aan wettelijke verplichtingen zoals voldoen aan NEN 7513. Als de logging nog

ontbreekt moet die uiteraard gerealiseerd worden. Als de logging er wel is maar bijvoorbeeld niet aansluit op de door NEN 7513 genoemde internationale codestelsels, dan moet die aansluiting alsnog worden gerealiseerd.

- *Door zorginstellingen:*

Zorginstellingen kunnen de leveranciers helpen om aan die verplichtingen te voldoen.

Dat begint met ondersteunen van de leverancier bij het prioriteit geven aan realisatie van logging die voldoet aan NEN 7513. Als een oude release niet voorziet in goede logging en een nieuwe wel dan moet een zorginstelling zo veel mogelijk overgaan naar die nieuwe softwarerelease en niet van de leverancier verlangen dat die oudere release ook wordt aangepast.

Overgaan op een nieuwe release kan echter onbetaalbaar worden als dan bijvoorbeeld een kostbaar apparaat zoals een MRI-scanner moet worden vervangen terwijl die scanner nog niet is afgeschreven. Zorginstellingen zouden als tijdelijke oplossing het aantal medewerkers met toegang tot de gegevens in dat systeem kunnen minimaliseren dan wel de bewaartijd van gegevens kunnen verkorten. Deze aanpak vereist dat de gegevens ook in het centrale ziekenhuisinformatiesysteem of cliënteninformatiesysteem worden geplaatst en dat is vaak het geval.

Bij aanschaf van nieuwe software of apparatuur is het verstandig om in overeenstemming met de nieuwe richtlijn voor Medical Devices die in 2020 van toepassing wordt, garanties te vragen van de leverancier voor de periode gedurende welke blijvend wordt voldaan aan de bestaande en nog niet bestaande beveiligingseisen in de zorg.

Bij software die al langer wordt gebruikt maar geen logging heeft, hebben zorginstellingen meerdere argumenten om de leverancier te overtuigen om in actie te komen.

Bij internationale leveranciers kunnen zorginstellingen erop wijzen dat logging geen Nederlandse hobby is en NEN 7513 is uitgegaan van internationale standaarden[19]

Van belang is ook dat de Autoriteit Persoonsgegevens recentelijk een flinke boete heeft opgelegd aan een zorginstelling wegens tekortschietend toezicht op de logging. Als het toezicht praktisch onmogelijk is door tekortschietend log, kunnen zorginstellingen proberen om dit soort financiële risico's geheel of gedeeltelijk af te wentelen op de partij waarvan zij afhankelijk zijn om die boete te voorkomen: de leverancier van de software.

Als de softwareleverancier ook verwerker is, kan de zorginstelling hiervoor een beroep doen op de bijstandsverplichting van art 28 AVG[20]. Als de softwareleverancier geen verwerker is, kan wellicht via een beroep op wanprestatie met verwijzing naar algemeen geldende normen de boeteschade worden verhaald. In beide situaties doet de zorginstelling er goed aan om actief, aantoonbaar en voordat de Autoriteit Persoonsgegevens op de stoep staat, de softwareleverancier te wijzen op de risico's die hij loopt als de zorginstelling een boete krijgt.

Tot een gang voor de rechter hoeft het niet te komen want voor leveranciers die verzoeken om aan de geldende regelgeving te voldoen, blijvend negeren, zou geen markt binnen de zorg mogen bestaan.

---

[1] Frederiek Weeda, Privacy brengt patiënt in gevaar, NRC, 7 oktober 2019, https://www.nrc.nl/nieuws/2019/10/07/privacy-brengt-patient-soms-in-gevaar-a3975942
Floor Bouma, Kabinet wil dat meer Nederlanders gegevens delen voor spoedgevallen, NRC, 30 oktober 2019, https://www.nrc.nl/nieuws/2019/10/30/kabinet-wil-optie-delen-medische-gegevens-voor-spoedgevallen-a3978491,

ANP Nieuws, Iedereen binnen EU toegang tot medisch dossier, AvroTros, 6 februari 2019, https://zorgnu.avrotros.nl/nieuws/item/iedereen-in-eu-toegang-tot-medisch-dossier/

[2] Michel van der Geest, Patiëntdossiers in te zien door lek bij ziekenhuis OLVG, Volkskrant 15 februari 2019 https://www.volkskrant.nl/nieuws-achtergrond/patientdossiers-in-te-zien-door-lek-bij-ziekenhuis-olvg~bab966c4/ , Lieke Jongbloed, Maatregelen na privacyschending Barbie, Telegraaf 5 april 2018 https://www.telegraaf.nl/nieuws/1876497/maatregelen-na-privacyschending-barbie

[3] Artikel 35 lid 2 Wbp impliceert logging evenals art 15 lid 1 onder c) AVG aangevuld met de verplichting van art 12 AVG om de informatie beschikbaar te stellen aan de betrokkene in "duidelijke en eenvoudige taal".

[4] Toegang tot digitale patiëntendossiers binnen zorginstellingen, Autoriteit Persoonsgegevens, juni 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-zorginstellingen.pdf

[5] Art 15a lid 1 Wabvpz: alleen met uitdrukkelijke toestemming van de patiënt mogen de gegevens worden opgenomen in een 'elektronisch uitwisselingssysteem' tussen zorginstellingen

[6] Art 15a lid 2 Wabvpz.

[7] Shanna Spoelstra, Wet gespecificeerde toestemming elektronische uitwisseling opgeschort, Skipr, 8 oktober 2019, https://www.skipr.nl/actueel/id39933-wet-gespecificeerde-toestemming-elektronische-uitwisseling-opgeschort.html, Kamerstukken II ,2019/2020, 27529, nr. 209, brief van de minister voor medische zorg met de voortgangsrapportage Wet Cliëntrechten bij elektronische verwerking van gegevens met op blz. 2 aankondiging van onderzoek naar gebruiksvriendelijke, juridisch houdbare manieren om toestemming te verlenen door de patiënt voor de inzage door de zorgverlener.

[8] VZGZ, Effecten en baten zorginfrastructuur, jan 2018, https://www.vzvz.nl/actueel/zorginfrastructuur-voorziet-groeiende-behoefte-bij-zorgverleners, blz. 34

[9] Norm voor Informatiebeveiliging in de zorg, NEN 7510:2011, blz. 83 onder 10.10.1 met verwijzing naar de norm voor "Vastleggen van acties op elektronische patiëntendossiers, NEN 7513" ("Loggingnorm"). Logging wordt ook expliciet in de Wabvpz genoemd in artikel 15e dat nog in werking moet treden. Lid 1 voor uitwisselingssystemen en lid 2 voor ieder systeem.

[10] Kamerstukken II ,2012/13, 33509, 3 (MvT bij Wijziging van de Wet cliëntenrechten zorg, de Wet gebruik Burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet), blz. 7 onder <<Logging>>.

[11] Liza van Lonkhuyzen, Jeroen Wester, Patiënten komen vaak niet te weten wie er in hun medische dossier neuzen, NRC, 25 oktober 2019, https://www.nrc.nl/nieuws/2019/10/25/patienten-komen-vaak-niet-te-weten-wie-er-in-hun-medische-dossier-neuzen-a3978116 en Liza van Lonkhuyzen Jeroen Wester, Wie gluren er allemaal in mijn medische dossier?, NRC, 25 oktober 2019, https://www.nrc.nl/nieuws/2019/10/25/wie-gluren-er-allemaal-in-mijn-medische-dossier-a3978083

[12] Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom, Autoriteit Persoonsgegevens, 18 juni 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf

[13] Norm voor Informatiebeveiliging in de zorg NEN 7510:2017, blz. 90 verwijst naar een SIEM.

[14]Jason Skowronski, 30 best practices for logging at scale, Blog op Solarwinds Loggly, 21 Jun 2017, https://www.loggly.com/blog/30-best-practices-logging-scale/. Goede performance bijvoorbeeld vereist een goede programmeringstechniek waarbij eerst de gebruiker inzage krijgt in de gevraagde gegevens waarna de loggegevens worden wegeschreven zonder de programma-uitvoering te blokkeren ("asynchroon").

[15] Staatscourant, 38007, 10 juli 2019, Besluit van de Minister voor Medische Zorg van 27 juni 2019, kenmerk 1529221-190512-WJZ, houdende vaststelling van een bewaartermijn voor logging, https://zoek.officielebekendmakingen.nl/stcrt-2019-38007.pdf

[16] Modelovereenkomst van de Vereniging Brancheorganisaties Zorg, art 4.2 tot en met 4.4, https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/

[17] Whitepaper over toepassing van informatiebeveiligingsnormen in het zorginkoopproces, https://www.nen.nl/Alles-over-NEN-7510.htm

[18] Als voorbeeld moesten zorginstellingen recentelijk Citrix uitzetten, zie Nu.nl, Citrixlek treft meer dan honderd zorginstellingen, 16 januari 2020, https://www.nu.nl/tech/6024323/expertisecentrum-citrix-lek-treft-meer-dan-honderd-zorginstellingen.html maar dat gevaar ligt op de loer bij wel meer software.

[19] NEN 7513:2018, blz. 21. Het betreft rfc3881, http://tools.ietf.org/html/rfc3881, Dicom Audit message Format, http://dicom.nema.org/medical/dicom/current/output/html/part15.html#sect_A.5 en ATNA/IHE Technical Framework, https://www.ihe.net/resources/technical_frameworks/

[20] Jaap van der Wel, Privacybescherming is niet gediend met starre wetsuitleg, Ned. Tijdschr. Geneeskd. 18 november 2019; https://www.ntvg.nl/artikelen/privacybescherming-niet-gediend-met-starre-wetsuitleg