White Paper: Juridisch kader voor het delen en opslaan van patiëntgegevens middels een mobiele berichtendienst

Inleiding: "appen" van patiëntgegevens

Artsen wisselen regelmatig patiëntgegevens uit. Omdat ze hun directe collega's willen informeren, omdat ze de mening van een vakgenoot willen horen om zo de patiënt beter te kunnen behandelen of om vakgenoten te wijzen op interessante gevallen.

Onlangs heeft de Autoriteit Persoonsgegevens er op gewezen[1] dat artsen de berichtendienst Whatsapp niet zouden moeten gebruiken voor het uitwisselen van patiëntgegevens. Ook de KNMG heeft daarvoor gewaarschuwd[2]. Bij het gebruik van Whatsapp spelen twee zaken: de beveiliging van de informatie die via de dienst wordt uitgewisseld en bewaard, en de vraag of informatie-uitwisseling via WhatsApp überhaupt is toegestaan onder de privacy regelgeving (Wbp, Wgbo). De beveiliging is bij Whatsapp problematisch.

Voor het via een veilige berichtendienst delen van patiëntinformatie, gelden, uitgaande van een afdoende beveiliging, de gewone regels omtrent geheimhouding. Dat zijn precies dezelfde regels die een medische professional toepast bij, bijvoorbeeld, telefonisch overleg of bij het uitwisselen van leerzame praktijkgevallen. Hieronder volgt een kort overzicht van die regels toegespitst op het gebruik van een berichtendienst. Daarbij geldt dat dat gebruik pas mogelijk is als die dienst afdoende is beveiligd.

Voor wie is deze white paper?

1. Artsen en andere zorgprofessionals
2. ICT professionals in de zorg
3. Besturen en adviseurs van zorginstellingen

Plan van behandeling

Hieronder treft u eerst een samenvattend schema aan.

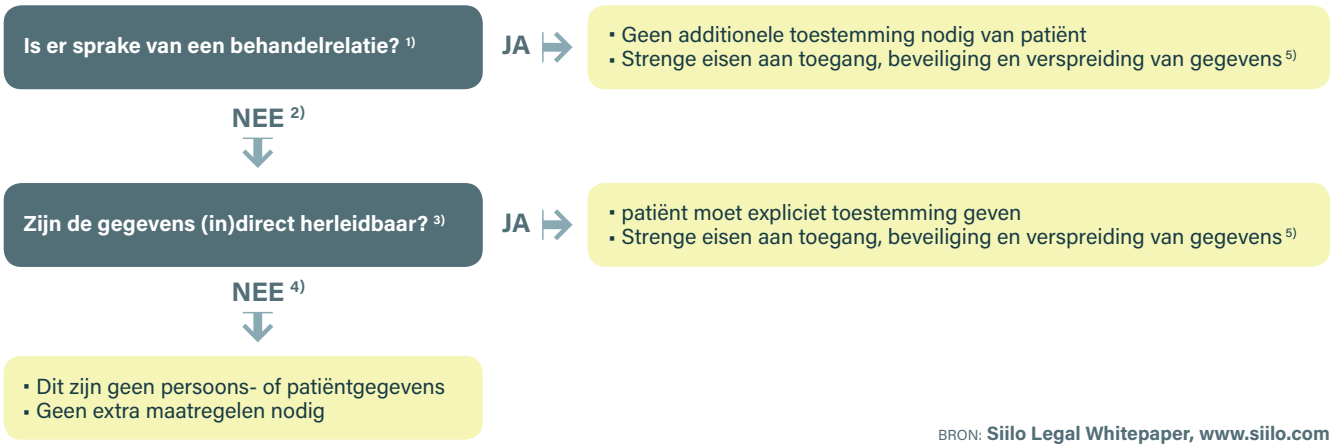
Daaronder komt de wettelijke regeling aan bod, daarna volgt een meer praktische uitwerking daarvan en een stuk over de beveiliging van het delen van gegevens via een berichtendienst. Ook gaan we kort in op de aanvullende verantwoordelijkheid van betrokken partijen onder de geldende privacyregelgeving. Tenslotte is er aan de hand van de uiteengezette juridische kaders een juridische toets van de "Siilo Messenger".

Dat wat geldt voor de arts, geldt voor iedere zorgprofessional.

[1] http://nos.nl/artikel/2088687-privacywaakhond-artsen-mogen-whatsapp-niet-meer-gebruiken.html
[2] http://www.knmg.nl/Diensten/KNMG-Artseninfolijn-10/Casus-Artseninfolijn/151855/Mag-een-arts-patientgegevens-uitwisselen-via-WhatsApp.htm

Samenvattend schema

Beslisboom bij het delen van patiëntgegevens met collega's over een messenger



BRON: **Siilo Legal Whitepaper, www.siilo.com**

VOETNOTEN

1) Collega's uit het behandelteam en zorgprofessionals daarbuiten waarvan redelijkerwijs kan worden gemeend dat een ieder daadwerkelijk aan de behandeling van de specifieke patiënt kan bijdragen
2) Bijvoorbeeld bij het delen van interessante praktijkgevallen (i.e. casuïstiek) met collega's
3) Indirect herleidbare gegevens zijn bijvoorbeeld gezichten, tatoeages en meta-data of combinaties daarvan
4) Siilo geeft de mogelijkheid (in)direct herleidbare kenmerken in foto's onomkeerbaar te anonimiseren, waarbij de meta-data (zoals tijdstip en locatie) automatisch worden gewist
5) Alle gegevens worden bij Siilo Messenger versleuteld verstuurd en opgeslagen bij verstuurder en ontvanger, inclusief gemaakte foto's met de telefoon

Wat zegt de wet over het delen van patiëntgegevens?

Drie wetten zijn van belang. In de Wet op de Beroepen in de Individuele Gezondheidszorg (Wet BIG) is het medisch beroepsgeheim opgenomen[3]. Het medisch beroepsgeheim wordt uitgewerkt in de Wet op de geneeskundige behandelingsovereenkomst (WGBO)[4], die ook de verhouding tussen u en uw patiënt regelt. Tenslotte is er de Wet bescherming persoonsgegevens (Wbp), die regelt hoe u met gezondheidsgegevens mag omgaan. Op de regels van de WGBO en de Wbp gaan we hieronder verder in. De Wet BIG vult het beroepsgeheim niet verder in en kan in dit kader verder onbesproken blijven.

De WGBO

Volgens de WGBO[5] mag u gegevens over een patiënt niet delen met anderen zonder toestemming van die patiënt. U heeft echter geen toestemming van de patiënt nodig[6] als u gegevens deelt met degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst, voor zover dat

[3] Art. 88 Wet BIG
[4] De Wet op de geneeskundige behandelingsovereenkomst is opgenomen als afdeling 5 (De overeenkomst inzake geneeskundige behandeling) van Titel 7 (Opdracht) van Boek 7 van het Burgerlijk Wetboek: art 7:446 tot en met 7:468 BW
[5] art. 7:457 lid 1 BW
[6] art. 7:457 lid 2 BW

noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden. Hieronder vallen in ieder geval de leden van het behandelteam in het ziekenhuis (de zogenoemde functionele eenheid[7]). Een collega-vakgenoot die door u wordt geraadpleegd met het oog op de behandeling van de patiënt kan doorgaans worden beschouwd als een persoon wiens medewerking beroepsmatig noodzakelijk is[8].

De Wbp

Patiëntgegevens zijn in de regel, omdat ze aan een identificeerbare persoon te koppelen zijn, persoonsgegevens in de zin van de Wbp[9]. Die koppeling aan een identificeerbare persoon kan direct zijn, een Burgerservicenummer bijvoorbeeld, of indirect. Denk daarbij aan een gegevens die een foto van een bijzondere wond bevatten en de metadata van een foto (tijd en plaats) die te combineren zijn met nieuws over een zwaar auto-ongeluk en zo identificatie van de persoon achter de wond mogelijk maken.

De Wbp regelt wat er wel en niet met die gegevens mag gebeuren. Medische gegevens zijn bijzondere persoonsgegevens[10], die alleen mogen worden verwerkt met toestemming van de patiënt[11], of, zonder diens toestemming, in het kader van de behandeling van de patiënt[12] of in levensbedreigende situaties[13]. Op die afzonderlijke situaties gaan we hieronder in.

Deze regels gelden *naast* de regels omtrent het beroepsgeheim. Dat betekent dat als het delen van patiëntgegevens volgens de Wbp kan maar in strijd is met het beroepsgeheim, dat delen toch niet mogelijk is.

In het kader van de behandeling

De Wbp staat, net als de WGBO, toe dat gegevens zonder toestemming van de patiënt, worden gedeeld met degenen die bij de behandeling betrokken zijn, als dat tenminste gebeurt met het oog op de behandeling (met andere woorden: als dat delen bijdraagt aan de genezing van de patiënt). Daaronder valt ook intercollegiale toetsing met dat doel door hulpverleners onderling[14]. Dit hoeven dus geen collega's te zijn die behandelingstoestemming hebben, maar collega's die ideeën kunnen hebben die de behandeling verder helpt.

Voor het delen van gegevens over interessante praktijkgevallen, dus buiten het kader van de behandeling, gelden andere regels, waarop hieronder zal worden teruggekomen.

Vitaal belang

[7] Zie daarover de gedragsregels van de KNMG
[8] Memorie van Toelichting bij wetsvoorstel WGBO, Tweede Kamer, vergaderjaar 1989-1990, 21 561, nr. 3, p. 39; zie ook College Bescherming Persoonsgegevens,Informatieblad Geheimhouding van medische gegevens, Informatieblad 33A, Februari 2011
[9] art. 1 sub a Wbp
[10] art. 16 Wbp
[11] art. 23 lid 1 sub a Wbp
[12] art. 21 lid 1 sub a Wbp
[13] art. 23 lid 1 sub d Wbp
[14] Memorie van Toelichting bij wetsvoorstel Wbp, Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3 p. 110

U heeft geen toestemming van de patiënt nodig om diens gegevens te delen met wie dan ook, als er sprake is van een dringende medische noodzaak om dat te doen. Het moet dan gaan om een zaak van leven of dood, bijvoorbeeld als onmiddellijk medische hulp nodig is naar aanleiding van een ongeval van de betrokkene waarbij deze buiten bewustzijn is geraakt[15]. Er kan dan nog geen behandelrelatie zijn omdat de patiënt in kwestie geen behandelrelatie kon aangaan: hij was bewusteloos.

Toestemming van de patiënt

Toestemming van de patiënt is wettelijk gezien de regel. Het zonder toestemming delen, dat hiervoor is besproken, is een wettelijke uitzondering op die regel. Als niet aan de voorwaarden voor het zonder toestemming delen wordt voldaan heeft u dus altijd toestemming van de patiënt nodig. In dat geval moet er sprake zijn van *uitdrukkelijke* toestemming van de patiënt voordat u zijn of haar gegevens kunt delen. Dit bepaalt de Wbp.

Uitwerking

In het kader van de behandeling

Binnen de hierboven geschetste kaders van de WGBO en de Wbp, mag u patiëntgegevens in het kader van de behandeling delen met collega's (in de functionele eenheid) en met vakgenoten zonder dat daarvoor toestemming van de patiënt nodig is.

Dat betekent niet dat bijvoorbeeld een foto van een bijzondere wond mag worden gedeeld in een groep van 20 willekeurig specialisten op dat gebied, in de hoop dat een daarvan kan bijdragen aan de genezing van de patiënt. De eis dat er alleen mag worden gedeeld in het kader van de behandeling, brengt met zich mee dat u redelijkerwijs moet kunnen menen dat degene met wie gedeeld wordt daadwerkelijk aan de behandeling van deze specifieke patiënt kan bijdragen, bijvoorbeeld omdat de betreffende arts al eerder door de behandelend arts in soortgelijke gevallen is geraadpleegd. U moet dus weten met wie u de gegevens deelt en u moet kunnen verantwoorden waarom u deelt. Een oncoloog uit Rotterdam mag dus wel gegevens betreffende zijn patiënt delen met collega's in Groningen, Genève en Helsinki die hij kent en van wie hij een concrete bijdrage kan verwachten. Hij mag die gegevens echter niet in een groep van 20 oncologen gooien in de hoop dat iemand hem kan helpen.

U, de individuele arts, blijft zelf verantwoordelijk voor de keuze van de vakgenoten met wie u patiëntgegevens deelt.

Toestemming van de patiënt

In alle andere gevallen, dient de patiënt uitdrukkelijke toestemming te geven voor het delen van zijn of haar gegevens.

[15] MvT Wbp Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3 p. 84

Dat betekent dat volstrekt helder moet zijn dat de patiënt begrijpt waarvoor hij toestemming heeft gegeven en dat hij die toestemming ook heeft willen geven. Toestemming 'om mijn gegevens te delen' is dus niet voldoende. De patiënt moet weten welke gegevens u wilt delen, met wie die gegevens gedeeld gaan worden en waarom. Een algemene toestemming aan de zorginstelling bij bijvoorbeeld de intake voldoet daar dus niet aan.

U kunt de patiënt vragen of u zijn foto via een app mag delen met 20 collega's om te zien welke van hen mogelijk een oplossing weet voor zijn of haar probleem. Als de patiënt daarop ja zegt, geeft hij uitdrukkelijk toestemming. Het moet dan nog steeds zo zijn dat het delen met die 20 collega's echt waarde kan hebben voor de patiënt. Als het ook met minder collega's kan, zult u daarvoor moeten kiezen.

De toestemming kan mondeling en schriftelijk worden gegeven, en zelfs impliciet zijn. Aangezien u de toestemming zult moeten bewijzen als de patiënt meent dat hij u die niet heeft gegeven, doet u er verstandig aan de toestemming vast te leggen.

U moet ervoor zorgen dat de patiënt zijn of haar toestemming vrij geeft. Het gaat erom dat de patiënt kan kiezen zonder dat er bij "nee" zulke grote negatieve consequenties volgen, dat hij wel "ja" móet zeggen. U moet voorkomen dat de patiënt zoveel druk ervaart dat hij of zij menselijkerwijs geen "nee" meer kan zeggen. Dan is de toestemming nietig.

Het delen van gegevens over interessante praktijkgevallen: toestemming

Het komt regelmatig voor dat artsen collega's willen wijzen op interessante praktijkgevallen, zonder dat dat direct bijdraagt aan de behandeling van de betreffende patiënt. Dat kan met uitdrukkelijke toestemming van de betreffende patiënt.

Het delen van gegevens over interessante praktijkgevallen: geanonimiseerde gegevens

Ontbreekt toestemming van de patiënt dan kunnen alleen gegevens gedeeld worden die nooit tot een patiënt te herleiden zijn. (teruggrijpen naar definitie patiëntgegevens) Gegevens zijn makkelijker tot een individu te herleiden dan men zou denken. Denk aan unieke tatoeages of aan wonden die direct in verband te brengen zijn met incidenten die in de media besproken zijn. Foto's bevatten vaak metadata (als plaats en tijdstip van de foto) die, gecombineerd met andere informatie, maken dat foto's tot een bepaalde patiënt te herleiden zijn. Datzelfde geldt voor metadata die in de gedeelde foto verborgen kunnen zitten, zoals plaats en tijd van de opname.

Het kan dus zijn dat u de foto moet bewerken om identificatie redelijkerwijs onmogelijk te maken. Dat kan door een tattoo of een gezicht te blurren en de metadata te verwijderen. Daar is software voor. Anonimiseren zal niet altijd mogelijk zijn. U blijft zelf verantwoordelijk voor het beoordelen van de vraag of er daadwerkelijk geen sprake meer is van (indirecte) persoonsgegevens (of patiëntgegevens?).

De Autoriteit Persoonsgegevens (AP) definieert [16] anonimisering als: doeltreffende technische en organisatorische maatregelen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Redelijkerwijs betekent zonder onevenredige inspanning. De anonimisering moet dus onder andere onomkeerbaar zijn.

Let op: het vervangen van namen of een identificerend nummer door een patiëntnummer dat alleen door u of uw instelling kan worden herleid tot een patiënt, is iets anders dan anonimiseren. Immers: iemand (u of uw instelling) kan vrij simpel dat patiëntnummer weer herleiden tot de patiënt zelf. Dit heet daarom pseudonimiseren. Gepseudonimiseerde gegevens zijn dus nog steeds persoonsgegevens. Vanzelfsprekend draagt pseudonimisering positief bij aan de beveiliging. Het is immers voor anderen dan u of uw instelling praktisch vrijwel onmogelijk de gepseudonimiseerde gegevens te herleiden tot een individu. Dat neemt niet weg dat voor de wet gepseudonimiseerde gegevens wel degelijk persoonsgegevens zijn en alleen geanonimiseerde niet meer.

Cryptografische bewerking van persoonsgegevens (zoals encryptie of hashing) speelt evenmin een rol als het gaat om de vraag in hoeverre gegevens al dan niet herleidbaar zijn tot de betreffende patiënt. Immers: degene die versleutelt kan nog steeds herleiden. Hiervoor geldt dus hetzelfde als bij de pseudonimisering is gemeld. Versleutelen pakt wel positief uit voor de beveiliging. Vanzelfsprekend is de impact van een hack veel kleiner als de buit bestaat uit goed versleutelde data. Daar hebben de hackers immers niets aan. De wetgever heeft bij de wetgeving rondom datalekken daaraan ook aandacht besteed. De meldplicht die de verantwoordelijke heeft in het geval van ernstige hack waarbij versleutelde gegevens in het spel zijn, is beperkt; bij zo'n hack hoeven de betrokkenen (in dit geval de patiënten) niet te worden ingelicht.

De conclusie is dus dat het delen van gegevens, buiten het kader van de behandeling, mogelijk is zonder toestemming van de patiënt als u er zeker van bent dat zijn of haar data voldoende zijn geanonimiseerd. En: alleen pseudonimisering is niet voldoende. En ook versleutelen is niet voldoende. Zij het dat beide technieken, pseudonimisering en versleutelen, de schade voor de patiënt bij een hack verkleinen.

Beveiliging van de gedeelde en opgeslagen gegevens

Het ontbreken van een adequate beveiliging was een van de grootste bezwaren van de AP en de KNMG tegen het gebruik van Whatsapp voor het delen van patiëntgegevens. De eis om adequaat te beveiligen volgt uit zowel de Wbp, de WGBO en de Wet BIG. Artikel 13 van de Wbp geeft globale handvatten voor die beveiliging die onder meer door de Autoriteit Persoonsgegevens zijn uitgewerkt[17].

[16] College bescherming persoonsgegevens: Onderzoek naar de verwerking van persoonsgegevens in het kader van de Nike+ Running app door Nike Inc., z2014-00859, OPENBARE VERSIE Rapport definitieve bevindingen, november 2015, p.86, waarin ook wordt verwezen naar Artikel 29-werkgroep, WP 216, Opinion 05/2014 on Anonymisation Techniques, 10 april 2014, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[17] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

De KNMG zegt over Whatsapp[18]: 'Weliswaar lijkt het juridisch toegestaan als die wordt gestuurd naar een collega-vakgenoot die door de arts wordt geraadpleegd met het oog op de behandeling van de patiënt. Die collega-vakgenoot kan dan worden beschouwd als een persoon die rechtstreeks betrokken is bij de uitvoering van de behandelingsovereenkomst. Daarvoor is geen toestemming van de patiënt nodig. Maar toch raden wij het af omdat de vertrouwelijkheid van de gegevensuitwisseling niet gegarandeerd is.'

De beveiliging van een berichtendienst speelt zich af op twee niveaus. Allereerst is daar de beveiliging van de gebruikte systemen en verbindingen die de berichtendienst ter beschikking stelt. Het andere niveau is dat van de telefoon.

Over de verbindingen en opslag stelt Whatsapp dat zij de gedeelde gegevens versleuteld en de berichten versleuteld bewaart op haar servers. Als die versleuteling er is en goed is uitgevoerd is dat een belangrijke stap in de goede richting.

Een bekend problemen is verder de onbevoegde toegang tot deze gegevens via de telefoon. De toegang tot WhatsApp en is niet beschermd met een pincode waardoor onbevoegden makkelijker toegang hebben tot patiëntgegevens die (vaak onnodig lang) op de telefoon staan. Toegang tot de telefoon betekent dan ook meteen toegang tot al die patiëntengegevens.

Dat probleem wordt vergroot doordat foto's van patiënten vaak makkelijk in de persoonlijke fotorol/galerij op de telefoon van de zorgprofessional terecht komen. Dit heeft twee hoofdoorzaken: WhatsApp plaatst standaard elk *ontvangen* foto in de persoonlijke fotorol of galerij. Dat is de standaard instelling. Die, overigens, kan worden uitgezet. Foto's die *genomen* worden met de standaard foto applicatie van de telefoon komen in elk geval altijd in de persoonlijke fotorol/galerij. Daar kan de gebruiker niets aan doen. Hij kan deze natuurlijk wel zo spoedig mogelijk verwijderen.

WhatsApp laat verder toe dat van de pushberichten, die op de telefoon binnenkomen, de eerste paar regels van een bericht vrij te lezen voor iedere (mee)kijker, ook al is de telefoon vergrendeld. Die eerste paar regels kunnen al gegevens bevatten die tot een patiënt te herleiden zijn.

Een ander probleem is dat de telefoon vaak synchroniseert met servers van derde partijen waarbij het de vraag is of die partijen hun beveiliging op orde hebben of dat die derde partijen overigens voldoende waarborgen bieden.

Verantwoordelijkheid

[18] http://www.knmg.nl/Diensten/KNMG-Artseninfolijn-10/Casus-Artseninfolijn/151855/Mag-een-arts-patientgegevens-uitwisselen-via-WhatsApp.htm

Als een berichtendienst een veilige manier biedt om patiëntengegevens te delen is het van belang te vermelden dat de gebruiker van de berichtendienst (de arts, en, als daarvan sprake is, de maatschap waar hij deel van uitmaakt of het ziekenhuis waar hij in dienst is) verantwoordelijk[19] is en blijft voor het naleven van de wettelijke regels, zoals geheimhoudingsplicht, beveiligingsplicht, informatieplichten, het niet langer bewaren van gegevens dan nodig is en het bieden van het recht van verzet aan de patiënt. Degene die de berichtendienst en de berichteninfrastructuur ter beschikking stelt is slechts bewerker[20] van de gegevens die de gebruiker wil delen, en doet dat onder diens verantwoordelijkheid. De verantwoordelijke en de bewerker zijn verplicht een zogenaamde bewerkersovereenkomst te sluiten.

Als de zorgverlener in dienst is van een maatschap of zorginstelling, is de maatschap of zorginstelling verantwoordelijke. De maatschap of de zorginstelling zal dan dienen te zorgen dat de omgang met de persoonsgegevens op een juiste manier geschiedt. Een correct gebruik van een veilige berichtendienst om te delen past binnen de nu al gebruikelijke omgang met patiëntengegevens. In zijn algemeenheid lijkt een aanvulling van de thans bestaande informatie (neergelegd in privacy statements) niet nodig. Dat kan echter anders zijn in een concreet geval. Een en ander is afhankelijk van de gekozen bewoordingen in de gehanteerde privacy documenten.

De zorgverlener die van een collega patiëntengegevens ontvangt is geen bewerker. Hij wordt zelf verantwoordelijke voor een juiste omgang met die gegevens. In de praktijk betekent dat dat hij die gegevens zodra zij niet meer nodig zijn, zal moeten deleten.

Juridische toets van "Siilo Messenger"

Siilo Messenger is een beveiligde berichtendienst. Siilo Messenger kan heel goed worden ingezet om binnen de hiervoor geschetste kaders patiëntengegevens uit te wisselen. Uitgangspunt voor ons als opsteller van dit white paper is dat Siilo de benodigde maatregelen heeft getroffen om de, met name hieronder, beschreven features correct en veilig uit te uitvoeren. En dat Siilo ook overigens adequaat en conform de wettelijke standaard (neergelegd in artikel 13 Wbp) is beveiligd. De technische controle als zodanig, gaat de bestek van dit white paper te buiten.

Dit zijn een aantal belangrijke communicatie- en beveiligingsfeatures van Siilo Messenger:

- Beveiliging bij het versturen van berichten (tekst, foto, video) voldoet aan alle zeven criteria van de EFF (Electronic Frontier Foundation) scorekaart [21] [22]

[19] art 1 sub d Wbp
[20] art. 1 sub e Wbp
[21] https://www.eff.org/node/82654
[22] de zeven criteria EFF scorekaart:
1. Alle communicatie van de gebruiker is versleuteld;
2. Alle berichten worden zodanig versleuteld dat ze onleesbaar zijn voor de provider (end-to-end-versleuteling);
3. Het is mogelijk om de identiteit te verifiëren van de personen met wie wordt gecommuniceerd;
4. Oude berichten zijn beveiligd als de sleutels zijn gestolen;
5. De broncode is beschikbaar voor onafhankelijk onderzoek op de aanwezigheid van fouten, achterdeuren en structurele beveiligingsproblemen;
6. De versleutelingsmethode is goed gedocumenteerd; en
7. De beveiliging is recentelijk (maximaal twaalf maanden terug) onafhankelijk geaudit.

- berichten (en de daarvan deel uitmakende foto's en video's) worden versleuteld opgeslagen bij verstuurder en ontvanger. De foto's en video belanden **niet** in de persoonlijke fotorol/galerij van de mobiel telefoon. Dit voorkomt WGBO en Wbp schendingen doordat derden die een onbeveiligde telefoon in handen krijgen niet bij deze foto's/video's kunnen. Ook voorkomt het het automatische syncen van de foto's en video's met derde partijen zoals Google en Apple;
- foto's kunnen onomkeerbaar worden geanonimiseerd. Daarbij worden ook de met een foto verbonden metadata gewist. Zie hiervoor voor een toelichting. Met behulp van Siilo Messenger correct geanonimiseerde foto's kunnen vrijelijk worden gedeeld;
- pushberichten die op een vergrendeld scherm van een telefoon verschijnen, geven niet de inhoud van het bericht weer. Daarmee wordt voorkomen dat "meekijkers" patiëntgegevens zien.

Siilo heeft verder onder meer de volgende (niet-technische) maatregelen genomen om ervoor te zorgen dat Siilo en de gebruiker in juridische zin voldoen aan de Wbp en WGBO:

- Siilo werkt als bewerker altijd conform een bewerkersovereenkomst met de verantwoordelijke. Bij het installeren van Siilo sluit de gebruiker een zogenaamde end user agreement én een (wettelijk verplichte) bewerkersovereenkomst met Siilo;
- Medewerkers en werknemers van Siilo zijn gebonden aan een geheimhoudingsovereenkomst;
- Siilo heeft een protocol om datalekken te melden;
- Siilo is verantwoordelijke als het gaat om de persoonsgegevens van haar gebruikers, i.e. de zorgprofessionals zelf, en heeft daarvoor de benodigde privacy policy's opgesteld en houdt zich aan die policy's.

Afsluiting

Deze white paper is geschreven onder verantwoordelijkheid van Jos Swinkels en Jetse Sprey van Versteeg Wigman Sprey Advocaten. Versteeg Wigman Sprey Advocaten is een advocatenkantoor dat in 2003 is opgericht door de drie naamgevers en gespecialiseerd is in privacy-, contract- en intellectuele eigendom vraagstukken.

Deze white paper geldt voor de huidige regelgeving en de stand van de jurisprudentie. Deze white paper is niet bedoeld als juridisch advies. Uitzonderingen op de hier weergegeven algemene regels kunnen van toepassing zijn. Voor de omgang met patiëntengegevens in concrete gevallen dient u zich tot een deskundige te wenden.

Versteeg Wigman Sprey Advocaten is niet verantwoordelijk voor de beoordeling van de technische en organisatorische beveiliging van Siilo en de aanwezigheid van de door Siilo genoemde features. De beoordeling daarvan komt voor rekening van Siilo en de door Siilo ingeschakelde deskundigen.

Amsterdam 10 mei 2016