Joost Bruggeman
arts en oprichter van Siilo, een beveiligde messenger-app voor de zorg

Sjaak Nouwt
beleidsadviseur gezondheidsrecht bij artsenfederatie KNMG

EIND-TOT-EINDVERSLEUTELING ALLÉÉN IS NIET GENOEG

Veilig appen doe je zo

Appen is een snelle en makkelijke manier om informatie over patiënten te delen. Maar hoe zorg je ervoor dat dat correct gebeurt? Joost Bruggeman en Sjaak Nouwt zetten de regels op een rij.

Het gebruik van een mobiele messenger-app is voor vier op de tien artsen niet meer weg te denken uit hun zorgpraktijk. Via een messenger-app, zoals WhatsApp, kan informatie over patiënten sneller en makkelijker worden gedeeld dan voorheen. Sinds WhatsApp eind-tot-eindversleuteling toepast op het berichtenverkeer (april 2016), zou je kunnen denken dat deze app nu geschikt is voor gebruik in de zorg. Maar dat is niet het geval.
Het is zaak om verder te kijken dan het beveiligen van alleen het berichtenverkeer. Want hoe verzorgt WhatsApp nu de opslag van foto's en berichten op de mobiele telefoon als ze eenmaal zijn afgeleverd? Waar en in welke vorm worden deze opgeslagen, en hoe is de opslag en de verdere verspreiding van de uitgewisselde gegevens beveiligd? Hoewel ú natuurlijk de automatische back-up van uw gesprekken én de synchronisatie met uw fotoalbum én clouddiensten heeft uitgezet (zie *figuur 1*), kunt u er wel zeker van zijn dat de ontvangers van uw berichten dit óók hebben gedaan?

Als u een messenger-app 'lege artis' wenst te gebruiken voor uw werk in de zorg, dan moet u handelen in overeenstemming met uw medisch beroepsgeheim (WGBO en Wet BIG) en met de algemene privacywetgeving (Wbp), maar hoe ziet dat er in de praktijk uit? Hieronder een drietal praktijkvoorbeelden om deze wettelijke kaders te verhelderen.

Voorbeeld 1
U wilt als huisarts foto's van een aandoening van uw patiënt via een messenger-app naar een behandelend medisch specialist sturen. U wilt overleggen over het te voeren beleid.

Voorbeeld 2
U bent specialist en u wilt overleg met een collega-specialist van een universitair medisch centrum over een mogelijke spoedinterventie. Uw patiënt heeft baat bij elke minuut tijdswinst en u stuurt daarom een filmpje van een CT-scan na het telefonisch overleg.

Voorbeeld 3
U bent als medisch specialist deelnemer in een gesprek met meerdere collega's op een messenger-app met wie u uitdagende casuïstiek bespreekt c.q. intervisie heeft. U legt een casus voor en heeft voor dit doeleinde ook foto's gemaakt van uw patiënt.

1. Criteria voor veilig gebruik

DATA IN TRANSPORT

Berichten versleuteld tijdens transport?	Berichten onleesbaar voor provider?	ID van de ontvanger verifieerbaar?	Oude berichten beveiligd?	Broncode beschikbaar voor inzage?	Versleuteling methode goed gedocumenteerd?	Beveiliging recentelijk geaudit?

Data in transport horen te voldoen aan alle zeven criteria van de EFF-Scorekaart. Ook data in rust horen goed beveiligd te zijn.

GETTY IMAGES

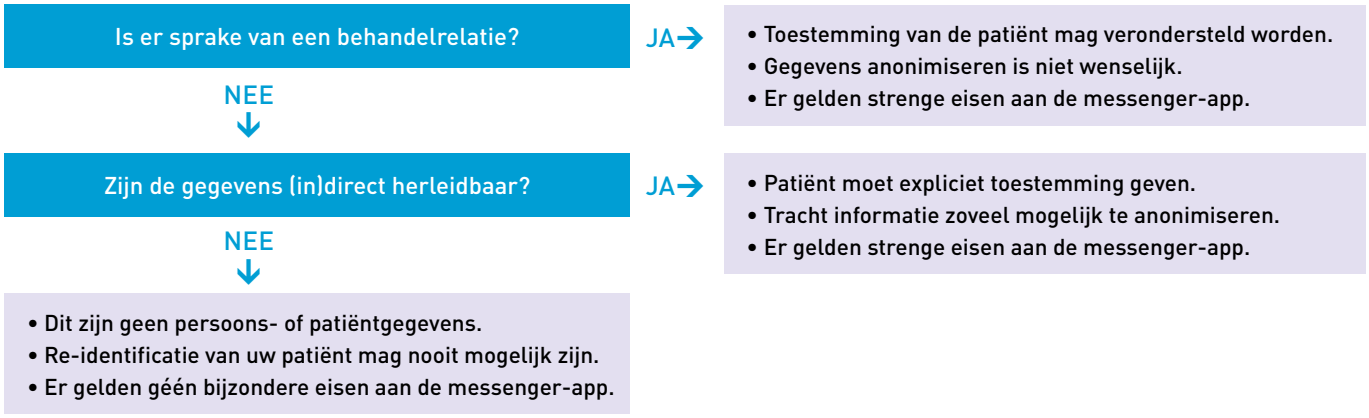
Het is zaak om verder te kijken dan het beveiligen van alleen het berichtenverkeer.

DATA IN RUST

Toegang tot berichten goed beschermd?	Berichten op telefoon ook versleuteld?	Hoe lang worden berichten bewaard?	Hoe synchroniseert de app met andere servers of apps?

Gegevens zijn makkelijker tot een individu te herleiden dan je zou denken

2. Wat wel en niet mag



Beslisboom om te bepalen hoe u met de gegevens van uw patiënt moet omgaan wanneer u deze wilt delen via een messenger-app.

Voordat u in uw rol als zorgverlener een messenger-app gebruikt, stelt u uzelf de volgende twee vragen (zie beslisboom in *figuur 2*):

Vraag 1: Heeft de ontvanger een behandelrelatie met mijn patiënt?
Als u in het kader van een overleg een bericht wilt sturen, dan moet u zich eerst afvragen of de ontvanger van uw bericht een behandelrelatie heeft met uw patiënt. Vanuit juridisch perspectief is er sprake van een behandelrelatie in de volgende gevallen:
- De hulpverlener heeft zelf een behandelingsovereenkomst met de patiënt.
- De hulpverlener is rechtstreeks betrokken bij de uitvoering van de behandelingsovereenkomst die een andere hulpverlener heeft met de patiënt.
- De hulpverlener is vervanger van de hulpverlener die een behandelingsovereenkomst heeft met de patiënt.

In voorbeeld 1 is sprake van een behandelrelatie, in voorbeeld 2 is dat goed mogelijk maar niet zeker en in voorbeeld 3 is er duidelijk géén behandelrelatie. De foto's en video's vallen onder het medisch beroepsgeheim van de arts die deze verstuurt via de messenger-app.

Vraag 2: Zijn de gegevens herleidbaar naar mijn patiënt?
De tweede vraag is: mag u, of moet u herleidbare informatie delen van uw patiënt? Een arts mag alleen tot diens patiënt herleidbare informatie aan een collega verstrekken in de volgende gevallen:[1]
- De patiënt heeft daarvoor uitdrukkelijk toestemming verleend.
- De arts stuurt de foto's naar een arts in het kader van een verwijzing, de patiënt is daarvan op de hoogte en heeft goedkeuring gegeven voor het delen van deze informatie.
- Een wet verplicht de arts tot het verstrekken van gegevens, bijvoorbeeld als een arts bij een patiënt een infectieziekte vaststelt.
- Een arts heeft serieuze aanwijzingen dat een patiënt zichzelf of anderen ernstige schade zal toebrengen, bijvoorbeeld als gevolg van psychische problemen.

De huisarts in voorbeeld 1 mag dus toestemming van de patiënt veronderstellen om herleidbare informatie te delen in het kader van de gezamenlijke behandelrelatie. Toestemming mag ook worden verondersteld als gegevens worden verstrekt aan de vervanger van de huisarts of specialist, of aan een ander die rechtstreeks betrokken is bij de uitvoering van de behandelingsovereenkomst, zoals een arts-assistent of doktersassistent. De verstrekking moet dan wel beperkt blijven tot die gegevens die noodzakelijk zijn voor de ontvanger om diens werkzaamheden te kunnen verrichten. De ontvanger echter, dient er wel zeker van te zijn dat de ontvangen informatie inderdaad bij uw patiënt hoort. Dat is immers de eerste vraag die u uzelf stelt wanneer u een röntgenfoto of ecg beoordeelt: 'Is dit het onderzoek van mijn patiënt?' Dus bij de uitwisseling van informatie via een messenger-app in het kader van een behandelrelatie geldt dat voor de ontvanger ook. Als in de besluitvorming geanonimiseerde informatie wordt uitgewisseld omdat u communiceert over een onveilig medium zoals WhatsApp, dan zal dat uiteindelijk tot misverstanden leiden, en zelfs tot wetsovertreding. U bent namelijk verantwoordelijk om de privacy van uw patiënt te beschermen (WGBO, Wbp) maar ook verplicht om uw patiënt op

de meest veilige en adequate manier te behandelen (Wet BIG).[2] Het kan dus belangrijk zijn dat de arts die de foto's stuurt, *juist* een naam en geboortedatum toevoegt aan het bericht. Om dan identiteitsfraude of een datalek te voorkomen, is het wel noodzakelijk dat u deze informatie via een messenger-app uitwisselt die voor deze gevoelige informatie beveiligd is.

Voorbeeld 2 is een veelvoorkomend scenario waarbij het vóór het sturen van de beelden nog niet vaststaat of de geconsulteerde arts een behandelrelatie zal krijgen met uw patiënt. Ervan uitgaande dat foto's herleidbaar zijn tot uw patiënt, en de ontvangende partij (nog) géén behandelrelatie heeft met uw patiënt, bent u strikt genomen verplicht om toestemming aan de patiënt te vragen voor het versturen van de foto's. Dat wil zeggen, uw patiënt moet *compos mentis* zijn, en op basis van volledige informatie uitdrukkelijk toestemming geven voor de uitwisseling van de foto's via de bewuste messenger-app. In acute situaties is het dikwijls een uitdaging om deze toestemming te verkrijgen. Wanneer u niet-herleidbare foto's en video's kunt sturen van uw patiënt, dan is deze toestemming niet verplicht, maar wel 'good practice'.

In voorbeeld 3 trekken we een parallel met het bespreken van casuïstiek in het kader van medisch onderwijs. In beginsel is het niet toegestaan om tot individuele patiënten herleidbare gegevens te delen met derden, ook niet voor onderwijsdoeleinden. Dat is namelijk een inbreuk op uw medisch beroepsgeheim en op de privacy van uw patiënt. Het is dus zeer belangrijk dat u de nodige voorzichtigheid aan de dag legt wanneer u details van uw patiënt bespreekt, en het is raadzaam om beeldmateriaal en beschrijvingen te anonimiseren.[3]

Anonieme gegevens

Als de gegevens die u verstuurt niet herleidbaar zijn naar uw patiënt, dan is verstrekking aan derden toegestaan. Schending van uw beroepsgeheim is dan ook niet aan de orde, maar wees bewust met wie en op welke manier u deze informatie deelt. Weet dat vandaag de dag niet snel sprake meer is van anonieme gegevens. De Autoriteit Persoonsgegevens (AP) definieert anonimisering als 'doeltreffende en organisatorische maatregelen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen zonder disproportionele inspanning is uitgesloten'. Anonimisering van patiënteninformatie moet naast volledig, namelijk ook onomkeerbaar zijn; na anonimisering mag re-identificatie niet meer mogelijk zijn. Gegevens zijn echter makkelijker tot een individu te herleiden dan je zou denken. Denk aan unieke tatoeages, of aan gevallen die direct in verband te brengen zijn met incidenten die in de media besproken zijn. Bovendien bevatten foto's vaak meta-data (zoals plaats en tijdstip van de genomen foto) die, gecombineerd met andere informatie, maken dat foto's tot een individu te herleiden zijn. Daarnaast worden hardware en software in de ICT niet alleen goedkoper en sneller, zij worden ook steeds slimmer door de combinatie van onze toenemende connectiviteit, de immer dalende prijs van dataopslag, 'big data'-analyse en toegepaste kunstmatige intelligentie.

Wanneer u niet-herleidbare foto's en video's kunt sturen van uw patiënt, dan is toestemming niet verplicht, maar wel 'good practice'

Lege artis

U kunt een messenger-app lege artis gebruiken als u goed weet met wie (vraag 1: behandelrelatie?) u welke informatie (vraag 2: herleidbaar?) deelt. Een arts die een foto verstuurt met inachtneming van de regels rond het medisch beroepsgeheim, de Wet bescherming persoonsgegevens en de Wet BIG, doet dat in overeenstemming met de wet als de messenger-app aan bepaalde voorwaarden voor de toegang, beveiliging en verspreiding van deze uitgewisselde gegevens voldoet (zie *figuur 1*). Bent u werkzaam in een organisatie, zoals een ziekenhuis, dan dient deze te weten hoe de informatie wordt verstuurd, hoelang en waar deze informatie wordt bewaard, en wie op welke manier toegang heeft tot deze informatie, en of deze informatie ook leesbaar is voor derden, zoals de provider van de messenger-app. Het is raadzaam om binnen uw organisatie, bijvoorbeeld bij de *information security officer*, na te vragen of het gebruik van een messenger-app door uw organisatie wordt toegestaan, en zo ja, welke. ■

contact
s.nouwt@fed.knmg.nl
cc: redactie@medischcontact.nl

Auteur Joost Bruggeman is oprichter van Siilo, een beveiligde messenger-app voor de zorg.

web

De voetnoten en eerdere MC-artikelen over dit onderwerp vindt u onder dit artikel op medischcontact.nl.