169.

WhatsApp in de zorg: veilig of niet?

SJAAK NOUWT

Veel artsen gebruiken WhatsApp in hun dagelijkse praktijk, bijvoorbeeld om onderling patiënten te bespreken of om juist met patiënten te communiceren. Ze versturen daarmee patiëntgegevens, waaronder foto's en andere gevoelige persoonsgegevens. Dat brengt privacyrisico's mee. Hoe groot zijn die risico's en zijn er alternatieven voor WhatsApp?

In 2016 bleek uit onderzoek onder het KNMG Artsenpanel dat 44 procent van de responderende artsen een messenger app, zoals WhatsApp, gebruikt voor werkgerelateerde doelen zoals het delen van patiëntgegevens met collega's.[1] Een derde daar weer van verstuurt 'wel eens' een foto, meestal van wonden of van de huid, voorzien van informatie over een patiënt. Het betreft dan dus tot individuele patiënten herleidbare gegevens die onder het medisch beroepsgeheim en andere privacyregels vallen.

Het privacyrisico hierbij lijkt misschien klein, zeker als patiënten er geen bezwaar tegen hebben gemaakt, of sterker nog, wanneer patiënten zelf vragen om via WhatsApp te mogen communiceren met hun arts. Er kan mogelijk veel gezondheidswinst worden behaald. Zo kunnen meerdere artsen die betrokken zijn bij een ingewikkelde transplantatie waarbij geen tijd mag worden verloren elkaar snel en eenvoudig informeren.

Toch heeft de Autoriteit Persoonsgegevens er bezwaar tegen. Zij riep artsen intussen op om op zoek te gaan naar alternatieven voor WhatsApp. Ook de KNMG adviseert artsen om geen foto's te versturen via WhatsApp, als die herleidbaar zijn tot individuele patiënten. Met name de beveiliging van persoonsgegevens en de elektronische communicatie daarvan lijkt niet in orde.[2] Artsen zelf zijn zich overigens – aldus het onderzoek – zeer bewust van de privacy- en beveiligingsrisico's.[3] Hoe onveilig is WhatsApp nu eigenlijk en zijn er voor artsen inmiddels veiliger alternatieven voorhanden? Daarover gaat dit artikel.

Scorekaart

De Amerikaanse digitaleburgerrechtenorganisatie EFF (Electronic Frontier Foundation) ontwikkelde een scorekaart voor de veiligheid van messenger apps.[4] Hoewel het onderzoek nog een vervolg krijgt, geven de resultaten tot nu toe al een indicatie van de veiligheid van messenger apps.

Die veiligheid wordt getoetst aan de volgende criteria:

1. Wordt alle communicatie van de gebruiker versleuteld?
2. Worden de berichten zodanig versleuteld dat ze onleesbaar zijn voor de provider (en-to-end-versleuteling)?
3. Is het mogelijk om de identiteit te verifiëren van de personen met wie wordt gecommuniceerd?
4. Zijn oude berichten beveiligd als de sleutels zijn gestolen? Dus wordt een eenmalig gebruikte sleutel na de communicatie meteen vernietigd?
5. Is de broncode beschikbaar voor onafhankelijk onderzoek op de aanwezigheid van fouten, achterdeuren en structurele beveiligingsproblemen?
6. Is de versleutelingsmethode goed gedocumenteerd?
7. Is de beveiliging recentelijk (maximaal twaalf maanden terug) onafhankelijk ge-audit?

Tot april 2016 lieten de scores van WhatsApp zien dat deze op vijf van de zeven getoetste criteria onveilig was:

1 Zie ook Heleen Croonen, 'Veilig whatsappen een must voor dokters'. *Medisch Contact* 25 november 2015, pag. 2314.

2 'Veiliger alternatieven voor WhatsApp', KNMG nieuwsbericht 23 maart 2016. Op internet: https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/veiliger-alternatieven-voor-whatsapp.htm.

3 KNMG, Mag een arts patiëntgegevens uitwisselen via WhatsApp? Praktijkdilemma 20 november 2015. Op internet: http://www.knmg.nl/Diensten/KNMG-Artseninfolijn-10/Casus-Artseninfolijn/151855/Mag-een-arts-patientgegevens-uitwisselen-via-WhatsApp.htm.

4 Electronic Frontier Foundation, Secure Messaging Scorecard, version 1.0. Op internet: https://www.eff.org/node/82654 (laatste update 5 april 2016). Omdat sommige van de zeven criteria moeilijk te meten zijn, werkt EFF op dit moment aan een nieuwe Secure Messaging Guide. Deze wordt binnenkort verwacht. Zie: https://www.eff.org/secure-messaging-scorecard (laatst geraadpleegd op 1 augustus 2016).

Maar sinds 5 april 2016 maakt WhatsApp gebruik van end-to-end encryptie. Daardoor zien de resultaten er nu heel anders uit:

Toch is WhatsApp hiermee mijns inziens nog niet veilig genoeg voor het versturen van patiëntengegevens. Met de invoering van een end-to-end encryptie zijn WhatsApp-berichten weliswaar uitsluitend nog te lezen voor de zender en ontvanger van dit bericht. En bijvoorbeeld niet voor het bedrijf WhatsApp Inc. Hiermee hebben de makers van WhatsApp een van de grote bezwaren tegen het zakelijk gebruik van de berichtenservice getackeld. De EFF scorekaart is eveneens op 5 april 2016 geüpdatet. Daarop scoort WhatsApp nu op 6 van de 7 beveiligingscriteria een voldoende. De broncode is echter nog altijd niet beschikbaar voor controle door onafhankelijke derden op de aanwezigheid van fouten, achterdeuren en structurele beveiligingsproblemen.

Omdat WhatsApp nog niet op alle punten veilig is, doen artsen er dus nog steeds verstandig aan te kiezen voor alternatieven die veiliger zijn.

De volgende min of meer algemeen bekende messenger apps zijn volgens deze scorekaart evenmin 100 procent veilig.[5] Ook zij scoren allemaal op twee of meer criteria negatief:

Alternatieve apps

De scorekaart laat ook zien dat er andere, mogelijk minder bekende messenger apps bestaan die wél op alle punten goed scoren, en dus veiliger communiceren dan WhatsApp. Dit zijn Off-The-Record Messaging for Windows (Pidgin), Signal[6], Silent Phone, Silent Text en Telegram (secret chats). Samen met enkele collega's heb ik geheel willekeurig de messenger app Signal van Open Whisper Systems getest op gebruiksvriendelijkheid. Signal wordt overigens aanbevolen en gebruikt door de Amerikaanse klokkenluider Edward Snowden.
Onze ervaringen zijn in het kort als volgt. Signal is gratis beschikbaar via de appstore van Apple en Google. Het gebruik ervan blijkt net zo eenvoudig als WhatsApp. Het uitwisselen van berichten, foto's, video's, groepen aanmaken, et cetera via Signal werkt op een vergelijkbare manier als WhatsApp. Het maakt daarbij niet uit of de zender en ontvanger over een iOS of Android-apparaat beschikt. Ook is het mogelijk om te bellen met Signal. Als de ontvanger een foto uit Signal wil opslaan op zijn telefoon, dan moet eerst op de foto worden geklikt, waarna deze kan worden 'gedeeld' door hem op te slaan in de filmrol. Er is dus altijd een actieve handeling van de ontvanger voor nodig. Foto's komen dan niet onbedoeld tussen de vakantiefoto's op de filmrol terecht.
Een mogelijk nadeel van het gebruik van een alternatieve messenger app is dat de ontvanger dezelfde app moet hebben geïnstalleerd. Maar hier kan een zorginstelling wellicht sturend in zijn. En zo'n app is in een handomdraai geïnstalleerd.

Het lijkt al met al verstandig om voor professionele doeleinden over te stappen op een veiliger messenger app. Misschien is dat ook wel zo praktisch. WhatsApp kan men dan gewoon lekker privé blijven gebruiken. Dat maakt ook meteen de scheiding duidelijk tussen persoonlijk en zakelijk ge-app.

Alternatieven voor de zorg

Intussen zijn er diverse initiatieven die specifiek voor de gezondheidszorg veiliger mogelijkheden bieden om mee te communiceren. Voorbeelden daarvan zijn Kanta Messenger, MD Linking en Siilo.

Kanta Messenger is een beveiligde berichtenservice voor op de mobiele telefoon en pc. Daarvan hebben wij in eerste instantie de veiligheid getoetst aan de EFF-criteria op basis van de beperkt beschikbare informatie over Kanta Messenger op internet. Vervolgens hebben wij onze analyse voorgelegd aan producent Topicus Zorg voor een reactie. Mede op basis daarvan kunnen we concluderen dat Kanta Messenger lijkt te voldoen aan zes van de zeven

5 Laatst geraadpleegd op 25 juli 2016.

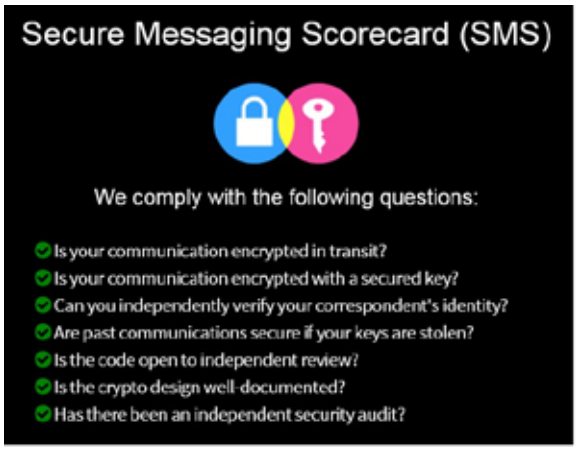
6 De messenger app Signal is de vervanger van de Android chat-app TextSecure en de Android bel-app RedPhone. Bron: Tweakers, 'Crypto-chat-app Signal vervangt TextSecure en RedPhone op Android', 3 november 2015. Op internet: http://tweakers.net/nieuws/106115/crypto-chat-app-signal-vervangt-textsecure-en-redphone-op-android.html.

EFF-criteria:[7]

1. Kanta maakt gebruik van end-to-end-encryptie.
2. Topicus heeft geen toegang tot de inhoud van de berichten.
3. De koppeling met contacten vindt plaats op basis van het scannen van een QR-code tijdens een fysieke ontmoeting. Daardoor weet de verzender altijd wie de ontvanger is.
4. Oude berichten zijn echter niet beveiligd als sleutels zijn gestolen. Als alternatief worden de data niet onbeperkt opgeslagen.
5. De broncode is beschikbaar voor review door partijen die security- en privacy-audits doen.
6. De werking van het hele protocol is gedocumenteerd.
7. De Kanta-server, iOS-app en Android-app zijn 'onlangs' door "Deloitte Assuring Medical Apps" op zowel privacy als security getest (datum onbekend).

MD Linking is sinds mei 2016 beschikbaar en profileert zich als een gratis en veilige messenger app, waarmee men college-artsen kan vinden en verbinden en dat de kwaliteit van de zorgverlening wereldwijd kan bevorderen.[8] MD Linking zou het eerste wereldwijde elektronische medische communicatiemiddel zijn. Het biedt mogelijkheden om kennis te delen (Educate), om met collega's via een beveiligde en versleutelde messenger app te communiceren (Communicate) en om collega's van over de hele wereld te vinden en mee te verbinden (Connect).

Volgens de (eigen) website van MD Linking voldoet deze messenger app aan alle criteria van de EFF Scorecard:



MD Linking is uitsluitend toegankelijk voor zorgprofessionals die werkzaam zijn in een zorginstelling ("all clinically practicing healthcare professionals globally"). Bij de registratie wordt gecontroleerd, bijvoorbeeld in het BIG-register, of de gebruiker wel een erkende zorgprofessional is.

Een derde voorbeeld is Siilo.[9] Ook voor gebruik van de Siilo medical messenger verifieert de Siilo Service Desk iedere gebruiker aan de hand van het BIG-register. Voor ieder gebruik van de app is een pincode of vingerafdruk nodig. Siilo maakt gebruik van end-to-end encryptie, waardoor berichten of foto's niet op een centrale server worden opgeslagen, maar alleen op het apparaat van de zender en ontvanger. De Service Desk heeft daardoor geen toegang tot de berichten en de afbeeldingen. De Siilo app biedt de mogelijkheid om herleidbare gegevens, zoals gezichten, namen, geboortedata of unieke lichaamskenmerken, te 'blurren' waardoor deze onherkenbaar worden. Berichten en foto's worden voorts automatisch gewist na 30 dagen. Mocht het apparaat verloren of gestolen worden, dan kunnen de gegevens van op afstand worden gewist van het apparaat.
Siilo heeft in april 2016 een onafhankelijke audit laten uitvoeren door Fox-IT, een bedrijf dat gespecialiseerd is in informatiebeveiliging. Daaruit zou volgen dat Siilo aan alle zeven beveiligingscriteria van EFF voldoet.

Er zijn nog wel meer messenger apps speciaal ontwikkeld voor gebruik in de gezondheidszorg. Te denken valt aan: Alterdesk, IQ secure messenger en Esculapp. Een nieuwe loot aan deze stam is KPN Zorg Messenger.[10] Deze heeft een e-mail en messenger functie, waardoor de gebruiker kan kiezen tussen e-mailen of appen. Zo kunnen artsen beide functionaliteiten volledig gescheiden of door elkaar gebruiken. Ook is het mogelijk om zelf in te stellen hoe lang de berichten op het apparaat van de gebruiker zichtbaar blijven. Berichten kunnen worden ingetrokken, waarna de ontvanger het niet meer kan zien. KPN verwacht deze dienst vanaf september 2016 aan te bieden.

Tot slot

WhatsApp is een zeer handig instrument dat wereldwijd door meer dan 1 miljard mensen wordt gebruikt. Ik vind het zelf ook een erg handige tool en ik gebruik het zowel privé als zakelijk. Het is dan ook niet vreemd dat artsen op een gegeven moment ook op het punt komen dat zij WhatsApp voor professionele doeleinden willen gebruiken. Wanneer men er echter gegevens over patiënten mee gaat uitwisselen moet men zich realiseren dat dit juridisch gezien een bijzondere (gevoelige) categorie van persoonsgegevens betreft. Bovendien vallen deze gegevens onder het medisch beroepsgeheim van de arts. Daarom is een goede beveiliging van deze gegevens en van de elektronische communicatie ervan, van groot belang. Daar zijn artsen zich in het algemeen ook goed van bewust.

7 Aldus ook de aanbieders van Kanta Messenger op https://www.kanta-messenger.nl/veelgestelde-vragen/ (laatst geraadpleegd op 1 augustus 2016).

8 https://mdlinking.com/static/homepage.html (laatst geraadpleegd op 25 juli 2016).

9 Zie ook: https://www.siilo.com/ (laatst geraadpleegd op 8 augustus 2016).

10 Yvonne Keijzers, 'Op weg naar een federatie rond veilig appen.' *ICT&Health*, nr. 03/2016, pag. 32-33.

Als gevolg daarvan schieten medische messenger apps tegenwoordig als paddenstoelen uit de grond. Een grote diversiteit aan medische messenger apps maakt dat er voor hulpverleners wel wat te kiezen valt. Maar aan dit brede aanbod zitten niet alleen voordelen. Want welke messenger app is de meest veilige en gebruikersvriendelijke? Voorts bestaat het risico dat hulpverleners die via een medische messenger app patiënteninformatie willen uitwisselen, niet over dezelfde messenger beschikken. Kan iemand die normaal gesproken Kanta Messenger gebruikt ook berichten ontvangen van een collega die Siilo gebruikt? Of moeten beide hulpverleners dan beide messenger apps op hun apparaat installeren? En geldt dat dan ook voor andere messenger apps die andere collega's weer gebruiken? Interoperabiliteit, oftewel het over en weer berichten kunnen uitwisselen tussen verschillende platformen, lijkt meer dan wenselijk. Dat geldt ook voor automatische koppelingen tussen messenger apps en de verschillende zorginformatiesystemen (HIS, ZIS, etc.). Enige coördinatie en standaardisatie op dit vlak lijkt mij daarom aangewezen en gewenst.

Over de auteur
mr. dr. S. (sjaak) Nouwt is beleidsadviseur gezondheidsrecht artsenfederatie KNMG. Dit artikel is op persoonlijke titel geschreven en is een bewerking van mijn artikel 'WhatsApp niet veilig, alternatieven wel', gepubliceerd in *Medisch Contact* 24 maart 2016. Op internet: http://www.medischcontact.nl/archief-6/Tijdschriftartikel/153276/WhatsApp-niet-veilig-alternatieven-wel.htm.
e-mail: s.nouwt@fed.knmg.nl
cc: zip@sdu.nl