GemsTracker General Privacy Impact Assessment

20 maart 2018

Inhoudsopgave

Samenvatting

In GemsTracker installaties worden van patiënten zowel persoonsgegevens als gegevens over hun aandoening, behandelgegevens en behandeluitkomsten opgeslagen in een streng beveiligde omgeving. Omdat een aantal installaties kwetsbare groepen betreft – kinderen met een geestelijke en/of lichamelijke beperking – is er veel aandacht besteed aan het beschermen van de privacy van de patiënten en het afdwingen van informed consent. Er wordt gebruik gemaakt van de software GemsTracker; de hosting voor de productieomgeving kan gebeuren binnen de eigen organisatie en bij elke NEN 7510 gecertificeerde hosting provider. CareFacts heeft hiervoor een overeenkomst bij TRUE.nl.

De toegang tot patiëntgegevens is organisatie specifiek en bij analyses van de gegevens wordt gewerkt met gepseudonimiseerde patiëntnummers die alleen met toegang tot de installaite gegevens herleid kunnen worden tot een patiënt.

De GemsTracker applicatie wordt regelmatig door externe bedrijven getest. Alle gevonden problemen worden altijd meteen opgelost.

De opslag van patiëntgegevens voor GemsTracker installaties voldoet aan de hoogst mogelijke normen van beveiliging.

Overzicht

Het doel van de GemsTracker software is het verzamelen van uitkomstmaten van patiënten voor zorgpaden en wetenschappelijk onderzoek om te komen tot een betere behandeling en behandeling op maat.

Gezien het privacygevoelige karakter van deze gegevens is de toegang tot de gegevens streng geregeld. GemsTracker slaat standaard alle gegevens in twee of drie databases op. Eén database bevat alle tot de persoon herleidbare informatie. Alle medische informatie wordt opgeslagen in een aparte database en is alleen te koppelen middels een gepseudonimiseerde sleutel.

De hele applicatie kent een sterk rollensysteem, waarbij het van iemand zijn rechten afhankelijk is wat ingekeken kan worden: bijvoorbeeld alleen patiënten van een bepaalde organisatie of zelfs dat niet als iemand alleen gepseudonimiseerde gegevens mag downloaden.

Bij de ontwikkeling van vragenlijsten en tracks wordt door onze consultants gekeken of mogelijk identificerende informatie wordt uitgevraagd in vragenlijsten en wordt gekeken of exports van data voldoen aan pseudonimiserings eisen zoals het lijstje van de HIPAA (http://cphs.berkeley.edu/hipaa/hipaa18.html).

De productieomgeving moet SSL gecertificeerd zijn. Een SSL certificaat is een bestand dat zorgt voor een betere beveiliging van gegevens tussen de server en een internet browser (als Chrome of Internet Explorer). Doordat SSL certificaten een beveiligde sleutel koppelen aan de connectie van een website kunnen gegevens versleuteld verzonden worden waardoor deze veilig ingevoerd kunnen worden zonder tussenkomst van externe systemen die de gegevens willen onderscheppen. Op dit manier kunnen persoonsgegevens veilig gebruikt worden op websites die beveiligd zijn met een SSL certificaat.

De servers waar deze gegevens op staan in een NEN 7510 gecertificeerde omgeving achter een zware firewall. Verkeer naar de servers kan alleen over de poorten voor HTTP en HTTPS, met uitzondering van speciale toegang voor beheerders. Beheerders van buiten het ziekenhuis netwerk moeten of (onder Linux) werken middels SSH verkeer over poort 22, wat alleen vanaf bepaalde IP adressen mogelijk is voor code updates, of (onder Windows) via VPN inloggen en Remote Desktop gebruiken.

Bij het bouwen van de applicatie is telkens rekening gehouden met het waarborgen van de privacy van de patiënten. Het gevolg is een applicatie met gelaagde beveiliging met pseudonimisatie en informed consent ingebouwd tot op het laagste niveau van gegevensopslag.

De applicatie bewaart het gedrag van de gebruikers en de applicatie en de server worden regelmatig extern getest op veiligheid.

De meldplicht datalekken voor alle partijen wordt vastgelegd in een aparte overeenkomst.

Het karakter van de informatie

GemsTracker slaat zowel persoonlijke gegevens over patiënten als informatie over hun aandoening, behandelgegevens en behandeluitkomsten op. Het gaat in GemsTracker vaak om het samenvoegen van reeds in de zorg te verzamelen data uit (al dan niet verschillende) ziekenhuizen t.b.v. het optimaliseren van behandelingen en het verbeteren van de kwaliteit van zorg.

Persoons identificerende informatie betreft BSN, patiëntnummer, naam, geboortedatum, postadres, email en telefoonnummers. Alleen patiëntnummer en email zijn noodzakelijk, de overige informatie wordt alleen opgeslagen indien deze door het ziekenhuis aangeleverd wordt en voor de zorg noodzakelijk is. Voor zover mogelijk en indien beschikbaar wordt deze informatie automatisch uit het EPD geïmporteerd.

De patiëntgegevens bestaan bijvoorbeeld uit leeftijd, lengte, gewicht en de medische voorgeschiedenis, bijkomende aandoeningen en diagnostische gegevens. Deze informatie kan, indien beschikbaar, automatisch uit EPD's geïmporteerd worden, en anders ingevoerd door de behandelaars, eventueel geassisteerd door een assistent.

GemsTracker werkt standaard met een patiëntnummer en een BSN nummer, voor zover deze bekend is. Indien een BSN opgegeven wordt voor een patiënt wordt alleen een one-way hash-waarde opgeslagen, zodat hiermee wel vergeleken kan worden, maar het BSN niet uit de applicatie opgehaald kan worden. Patiënten die vanwege verhuizing of doorverwijzing in meerdere centra worden gezien komen maar één keer in GemsTracker voor. Hun data worden – al dan niet tijdelijk - beschikbaar gesteld aan een ander centrum. Dit wordt geregeld in GemsTracker.

De gepseudonimiseerde gegevens worden samengevoegd op geaggregeerd niveau voor rapportages.

BSN opslag

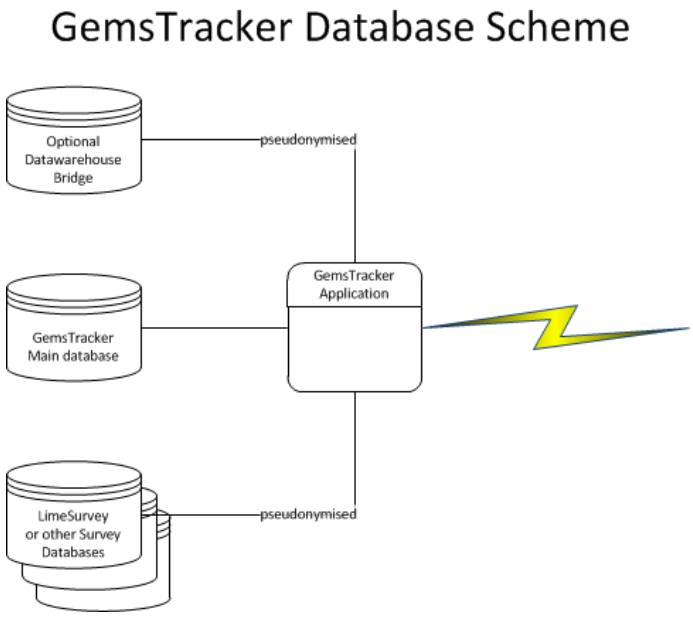
In plaats van het BSN zelf wordt een one-way hash van het BSN opgeslagen. Aangeleverde patiënten worden alleen op de hash met elkaar vergeleken. Toegang tot het systeem geeft dus nooit toegang tot de betreffende nummers en er kan ook niet op BSN gezocht worden,

Gebruik van de informatie

Technisch gebruik

GemsTracker slaat standaard de identificerende gegevens op in een hoofd-database en de diagnostische gegevens in een aparte database met een gepseu-donimiseerde identificatie. Toegang tot beide databases is vereist om beide gegevens te kunnen combineren.

Het schema rechts geeft een algemeen overzicht van de database structuur van GemsTracker. Zonder toegang tot de hoofd GemsTracker database zijn de diagnostische gegevens niet te herleiden



tot een patiënt. Standaard kan dit alleen via de GemsTracker applicatie, waarin per database een aparte gebruiker gedefinieerd kan worden.

Pseudonimisatie wordt ook gebruikt indien de gegevens opgeslagen worden in de optionele datawarehouse bridge, die te zien is in het schema bovenaan.

Toegang van personen

GemsTracker is alleen toegankelijk voor personen met een medewerker account. Elk account is gekoppeld aan een gebruikersgroep die bepaalt waartoe de gebruiker toegang heeft. De hele applicatie kent een sterk rollensysteem, waarbij het van iemand zijn rechten afhankelijk is wat ingekeken kan worden. Zo hebben behandelaars alleen toegang tot de gegevens van patiënten van hun eigen organisatie, maar kunnen ze die alleen op het scherm bekijken en niet exporteren. Omgekeerd hebben gegevensexporteurs weer geen toegang tot de individuele gebruikers. Voor hen worden er alleen gepseudonimiseerde gegevens gedownload. Alleen een kleine groep beheerders en supergebruikers hebben toegang tot alle patiënten. Ook kunnen zij de gegevens exporteren.

Wachtwoordbeleid

Voor de wachtwoorden van gebruikers geldt een standaardbeleid waarbij niet alleen vertrouwd wordt op een afwisseling van tekens, maar waarbij ook gebruik gemaakt wordt van een lijst met meest voorkomende, waardoor wachtwoorden zoals ‘Welkom01!” niet toegestaan zijn.

Gegevensexport

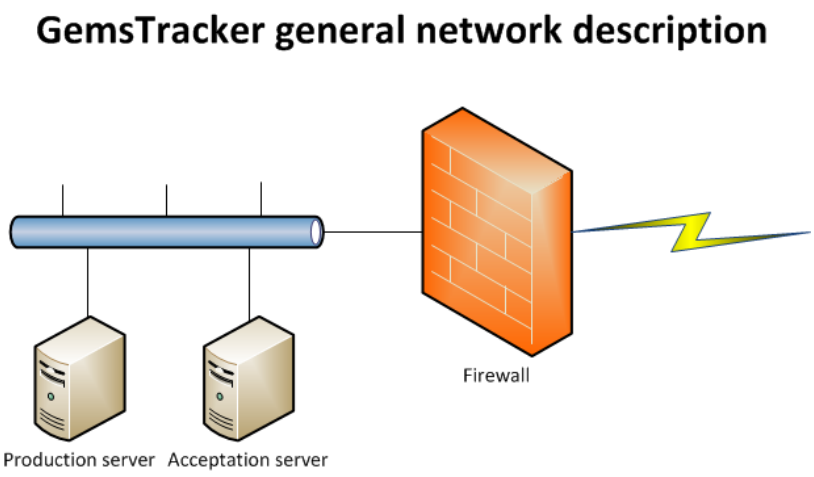
GemsTracker en LimeSurvey kunnen beiden gegevens exporteren voor gebruik in statistische pakketten zoals Stata, SPSS, R en Excel. Dit betreft altijd gepseudonimiseerde gegevens. Men moet de juiste toegangsrechten hebben om dit te kunnen.

Gegevensimport

Op dit moment is alleen handmatige import van patiënt, afspraak en medische gegevens mogelijk. Automatische import van gegevens gebeurt bij andere GemsTracker installaties, maar is nog niet mogelijk bij GemsTracker zonder de code aan te passen. De code aanpassingen om dit bij GemsTracker mogelijk te maken kunnen zeer beperkt zijn, echter: zonder een uitgebreid nieuw administratief goedkeuringstraject waarbij security en privacy nogmaals onder de loep genomen worden is dit niet te implementeren.

Inrichting van de beveiliging

Gegevens van echte patiënten worden alleen gebruikt op de GemsTracker productie en acceptatie servers. Op deze servers draait zowel de database applicatie als de webserver applicatie. Beide servers moeten achter een firewall staan ingericht in een NEN 7510 gecertificeerde netwerkomgeving.



Standaard laat de server alleen

HTTP en HTTPS verkeer door naar de servers, waarbij alle HTTP berichten automatisch naar HTTPS omgezet worden.

Beheerderstoegang

Naast toegang via de GemsTracker gebruikersinterface is er soms ook toegang tot de database door middel van phpMyAdmin. Deze toegang is alleen beschikbaar voor sommige medewerkers vanaf hun bedrijfsnetwerk en voor Jasper van Gestel en Matijs de Jong indien zij werken vanaf hun werkplekken, gecontroleerd op IP-adres door de firewall.

Daarnaast kunnen Jasper en Matijs meestal inloggen met SSH en SFTP vanaf dezelfde IP adressen of via VPN en Remote Desktop. Zij hebben echter geen root rechten tot de server, maar een beperkte gebruikerstoegang om de software bij te kunnen werken.

Informed consent (IC)

Bij de verzameling van persoonsgegevens is het noodzakelijk patiënten om toestemming te vragen de gegevens op te slaan en te bewerken voor specifieke doeleinden. Het GemsTracker platform biedt de mogelijkheid om per patiënt en organisatie voor elke uitgevraagde vragenlijst de IC status in te stellen. Bij de export van data wordt hier rekening mee gehouden: gegevens waarvoor geen IC aanwezig was, worden standaard niet geëxporteerd.

Alle patiënten moeten schriftelijk, tijdens het spreekuur, IC geven voor de gegevensopslag. Ondertekende consent formulieren worden in elk ziekenhuis opgeslagen.

Omdat het GemsTracker onderdeel is van de zorgpraktijk kunnen ook patiënten die geen IC hebben gegeven voor zorgdoeleinden opgenomen worden. Gegevens van deze patiënten (IC op “nee”) worden niet meegenomen in de export van gepseudonimiseerde data.

Bezwaarprocedure

Patiënten die wel IC hebben gegeven, kunnen deze te allen tijde intrekken. GemsTracker biedt 2 mogelijkheden in het geval een patiënt wil stoppen:

1) een patiënt stopt met deelnemen, maar trekt het IC niet in. In dit geval blijven de data behouden en ook beschikbaar in de gepseudonimiseerde export.

2) een patiënt trekt zijn/haar IC in: de data worden verwijderd uit de dataset. Alle gegevens die echter op geaggregeerd niveau zijn verwerkt kunnen daar niet meer uit worden verwijderd. TRUE hanteert een retentieperiode van 28 dagen alvorens een back up wordt overschreven. Dit betekent dat zodra een patiënt definitief wordt verwijderd uit GemsTracker zijn/haar data nog 4 weken aanwezig blijven in de back up.

Indien een patiënt stop met deelname aan de studie dan kan dat met of zonder intrekking van het IC. In beide gevallen wordt de patiënt zodanig gemarkeerd dat alleen beheerders nog bij de gegevens kunnen.

Indien het informed consent ingetrokken wordt, worden de invoergegevens zodanig gemarkeerd dat er geen onderscheid gemaakt kan worden tussen deze gegevens en onjuist ingevoerde gegevens. Vanaf dat moment zijn de gegevens ook niet meer beschikbaar in de gepseudonimiseerde export.

Tot slot kan de patiënt verzoeken om verwijdering van al zijn/haar gegevens. Hiervoor bestaat nog geen software oplossing. In de praktijk betekent dit dat Jasper van Gestel of Matijs de Jong deze gegevens handmatig uit de database zal moeten verwijderen. De reden hiervoor is dat er nog niet

een dergelijk verzoek geweest is in een GemsTracker installatie. Op het moment dat dit regelmatig voorkomt zal hier ongetwijfeld een softwareoplossing voor komen.

Gegevensbewaartermijn

Er is geen geplande gegevensbewaartermijn. Omdat we patiënten over de jaren blijven volgen (follow up systeem), blijft het register doorlopen; het is in principe niet eindig. Dit is pas van toepassing wanneer we bijvoorbeeld een nieuw systeem gaan gebruiken.

Auditing

Auditing applicatie toegang

De hele GemsTracker applicatie is auditable: alle gegevenswijzigingen worden geregistreerd, maar ook inloggen, uitloggen en het bekijken van patiëntgegevens.

Auditing kan aan- en uitgezet worden per onderdeel, maar ook dat wordt geregistreerd.

Audit gegevens kunnen eenvoudig per patiënt en per medewerker bekeken en geanalyseerd worden, als mede als geheel. Export van de gegevens naar Excel, CSV en SPSS is ook mogelijk.

Alle acties van gebruikers binnen GemsTracker kunnen worden gelogd en daarmee ook ge-audit worden. Standaard staat dit aan voor alle wijzigingen en voor het inkijken van patiënten.

Software audits & penetratie testen

De GemsTracker software, wordt geregeld getest door verschillende externe bureaus. Hierbij is de applicatie o.a. getest op de OWASP top 100 van kwetsbaarheden en daarin bestendig gevonden. Ook zijn test uitgevoerd waarbij de testers informatie van ontwikkelaars kregen over de architectuur van het systeem. Er is dus niet alleen getest met automatische penetratietesten, maar ook met testers (white hat hackers) die naar de code keken en zij getracht hebben binnen de applicatie de beveiliging te breken met gerichte aanvallen.

Alle tot nu toe gevonden serieuze kwetsbaarheden in de software zijn binnen 24 uur na rapportage opgelost. Sowieso konden deze kwetsbaarheden alleen gebruikt worden door gebruikers die al konden inloggen zoals de Research Nurses. Kwetsbaarheden voor mensen met patiënt toegang of minder zijn nooit gevonden. De reden hiervoor is dat de beveiliging op het laagste niveau van de applicatie gecontroleerd wordt, voor een al dan niet toegestane actie uitgevoerd kan worden.

Over het algemeen geldt dat de ernst van de gevonden kwetsbaarheden afnam met elk volgende testronde. Na de laatste testronde waren zelfs de minst belangrijke kwetsbaarheden uit de OWASP top 100 gedekt. De beveiliging van GemsTracker heeft de kwalificatie “paranoïde” gekregen, oftewel het hoogst mogelijke niveau van beveiliging.

Volgende tests staat al gepland voor januari 2018 en januari 2019. Deze tests worden uitgevoerd op de Reward GemsTracker installaties van Celgene Pharmaceuticals. Hun servers worden ook bij TRUE gehost. Daarnaast is de verwachting dat dit jaar nieuwe testrondes van de Pulse GemsTracker installaties van Equipe Zorgbedrijven uitgevoerd worden, maar hier is nog geen datum voor.

Server audits

Met de software audits worden ook altijd server audits uitgevoerd. Bij TRUE zijn hierbij tot nu toe geen problemen ontdekt.