GemsTracker Security

Er valt heel veel te vertellen over security van softwareapplicaties. Hieronder de belangrijkste punten met betrekking tot de beveiliging van de GemsTracker software en de bescherming van opgeslagen persoonsgegevens.

1 Penetratie testen

De GemsTracker software wordt geregeld aan tests onderworpen door verschillende testbedrijven. GemsTracker implementaties zijn getest bij verschillende hosting partijen. Na de laatste test ronde zijn we tegen alle bedreigingen uit de OWASP top 100 beschermd.
Hierbij is niet alleen getest met automatische penetratietesten, we hebben ook testers (white hat hackers) naar onze code laten kijken waarbij zij getracht hebben binnen de applicatie de beveiliging te breken met gerichte aanvallen. Alle lekken die in het verleden gevonden zijn waren binnen 24 uur gedicht en nooit is er een lek gevonden waarbij iemand zonder al bestaande inlogcode kon penetreren.

2 Privacy bescherming

GemsTracker slaat standaard alle gegevens in 2 of drie databases op. Één database bevat alle tot de persoon herleidbare informatie. Alle medische informatie wordt opgeslagen in aparte database en is alleen te koppelen middels een gepseudonimiseerde code.
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 gepseudnonimiseerde 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).

3 Informed consent

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

4 Auditing

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.

5 NEN 7510 certificering

Deze NEN norm is voor dataveiligheid in de zorg. De gehoste omgeving moet NEN 7510 gecertificeerd zijn om te voldoen aan de norm die als ziekenhuis geld. De applicatie binnen die omgeving hoeft niet apart getest te worden - mits er maar aantoonbaar aan de veiligheid gedacht is volgens best practices zoals omschreven in de NEN 7510 norm.
Een aparte normering van de applicatie is mogelijk bij voor een implementatie bij een enkele organisatie maar is duur en betekent met name dat veel tijd gestoken moet worden in het verder procedureel vastleggen van alle mogelijke gebruikersacties en daarbij behorende risico's.