Bewerkersovereenkomst

Partijen

Opdrachtgever, verder te noemen Praktijk,

en:

Health-e bv i.o. gevestigd aan het WG-plein 369, 1054 SG te Amsterdam en ingeschreven bij de Kamer van Koophandel onder dossiernummer 60417633, rechtsgeldig vertegenwoordigd door de heer De Casparis, directeur, verder te noemen HelloFysioApp,

in aanmerking nemende dat:

A. Praktijk een communicatieplatform en kennisbank in de vorm van een webapplicatie (verder "Portal"), ontwikkeld door HelloFysioApp, in gebruik wenst te nemen.
B. Praktijk en HelloFysioApp hiertoe een Overeenkomst hebben gesloten.
C. In het kader van die Overeenkomst verwerkt HelloFysioApp Persoonsgegevens, verkregen door Praktijk.
D. In deze Bewerkersovereenkomst zijn de afspraken die gemaakt zijn tussen Praktijk en HelloFysioApp over het verwerken van de Persoonsgegevens vastgelegd.
E. In aanvulling op het bepaalde in de Overeenkomst, komen Partijen in het licht van artikel 15 Wbp het volgende overeen.

Artikel 1. Definities

1.1 In deze Bewerkersovereenkomst hebben de volgende begrippen, steeds aangeduid met een hoofdletter, zowel in enkelvoud als in meervoud, de volgende betekenis:

a. *Betrokkene:* Degene op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in art. 1 sub f Wbp;
b. *Bewerker:* De bewerker als bedoeld in art. 1 sub e Wbp. In deze Bewerkersovereenkomst HelloFysioApp;
c. *Bewerkersovereenkomst*: Deze bewerkersovereenkomst, welke onlosmakelijk onderdeel uitmaakt van de Overeenkomst, ter neerlegging van de afspraken zoals bedoeld in art. 15 Wbp;
d. *Overeenkomst*: Het geheel van de tussen Praktijk en HelloFysioApp gesloten overeenkomsten inclusief bijlagen ten behoeve van ingebruikname van het Portal;
e. *Lek:* Verlies of ongeautoriseerde verwerking van Persoonsgegevens, of het bekend worden van een gebrek in de beveiliging die een aanmerkelijk risico daarop teweegbrengt;
f. *Partijen*: Praktijk en HelloFysioApp;

g. *Persoonsgegevens*: Gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon, zoals bedoeld in art. 1 sub a Wbp;
h. *Verantwoordelijke*: De verantwoordelijke als bedoeld in art. 1 sub d Wbp. In deze Bewerkersovereenkomst Praktijk;
i. *Verwerking*: Elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van Persoonsgegevens, zoals bedoeld in art. 1 sub b Wbp;
j. *Wbp*: Wet bescherming persoonsgegevens.

Artikel 2. Duur en beëindiging

2.1 Deze Bewerkersovereenkomst komt tot stand door ondertekening van Partijen op de datum van de laatste ondertekening.
2.2 Deze Bewerkersovereenkomst eindigt van rechtswege op het moment dat de langstlopende Overeenkomst eindigt.
2.3 Zodra de Bewerkersovereenkomst is beëindigd, is HelloFysioApp verplicht Praktijk binnen een maand na de beëindigingsdatum alle data inclusief Persoonsgegevens terug te bezorgen en deze te (laten) vernietigen op haar eigen systemen of de systemen van door haar ingeschakelde derden.

Artikel 3. Reikwijdte van Bewerkersovereenkomst en Verwerking door HelloFysioApp

3.1 HelloFysioApp zal de Persoonsgegevens die ter beschikking worden gesteld enkel verwerken met het oog op de uitvoering van de Overeenkomst.
3.2 Praktijk stelt de doeleinden vast voor de Verwerking van Persoonsgegevens. HelloFysioApp verwerkt Persoonsgegevens in opdracht van Praktijk uitsluitend met als doel het faciliteren van het Portal.
3.3Praktijk stelt HelloFysioApp op de hoogte van verwerkingsdoeleinden voor zover deze niet reeds in deze Bewerkersovereenkomst zijn genoemd. HelloFysioApp zal de Persoonsgegevens niet voor een ander doeleinde Verwerken dan door Praktijk is vastgesteld.
3.4 HelloFysioApp Verwerkt de gegevens uitsluitend binnen de Europese Unie.
3.5 HelloFysioApp is louter verantwoordelijk voor de Verwerking van Persoonsgegevens via de door haar onder de Overeenkomst aangeboden dienst onder de in de Bewerkersovereenkomst genoemde voorwaarden. Voor de overige Verwerkingen van Persoonsgegevens, waaronder in ieder geval begrepen maar niet beperkt tot de verzameling van de Persoonsgegevens door Praktijk en/of derden, is HelloFysioApp uitdrukkelijk niet verantwoordelijk.
3.6 De verantwoordelijkheid voor de Persoonsgegevens die met gebruikmaking van een door HelloFysioApp verleende dienst worden Verwerkt, ligt uitsluitend bij Praktijk. Praktijk staat er jegens HelloFysioApp voor in dat de inhoud, het gebruik en/of de Verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

3.7 Praktijk garandeert de naleving van de in de Overeenkomst genoemde afspraken, waaronder in ieder geval begrepen maar niet beperkt tot de daarin genoemde besluiten, overeenkomsten en wet- en regelgeving.

Artikel 4. Beveiliging

4.1 HelloFysioApp zal zorgen voor een adequaat niveau van beveiliging van de door haar verwerkte Persoonsgegevens tegen misbruik en ongeautoriseerd gebruik.
4.2 Partijen komen overeen dat HelloFysioApp voldoende technische en organisatorische maatregelen zal nemen met betrekking tot de te verrichten Verwerkingen van Persoonsgegevens tegen verlies of tegen enige vorm van onrechtmatige Verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de gegevens).
4.3 HelloFysioApp garandeert in ieder geval de maatregelen te hebben genomen die zijn genoemd in het Beveiligingsprotocol, welke in goed overleg tussen Partijen tot stand is gekomen en welke als bijlage is aangehecht aan deze Bewerkersovereenkomst. HelloFysioApp mag het Beveiligingsprotocol, wanneer dat eenmaal is vastgesteld, op ieder moment eenzijdig aanpassen, maar alleen zonder het niveau van de beveiliging te verminderen. HelloFysioApp zal Praktijk steeds op de hoogte stellen van aanpassingen.
4.4 Praktijk is verantwoordelijk voor de naleving van de door Partijen genomen maatregelen.
4.5 HelloFysioApp staat er niet voor in dat de beveiliging onder alle omstandigheden doeltreffend is. Indien een uitdrukkelijk omschreven beveiliging in deze Bewerkersovereenkomst ontbreekt, zal de beveiliging voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de Persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten niet onredelijk is.
4.6 Op eerste verzoek van HelloFysioApp zal Praktijk HelloFysioApp binnen 2 werkdagen schriftelijk informeren over de wijze waarop Praktijk uitvoering geeft aan haar verplichtingen op grond van de wet- en regelgeving op het gebied van de bescherming van Persoonsgegevens, waaronder in ieder geval begrepen de Wbp.

Artikel 5. Audits

5.1 Praktijk heeft het recht om periodiek audits uit te (laten) voeren ter controle van de afspraken onder deze Bewerkersovereenkomst.
5.2 HelloFysioApp zal de voor de audits benodigde ondersteunende gegevens zoals systeemlogs bewaren.
5.3 De personen die de audit uitvoeren zullen zich conformeren aan de beveiligingsprocedures zoals die bij HelloFysioApp van kracht zijn.
5.4 HelloFysioApp zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie zo tijdig mogelijk ter beschikking stellen.
5.5 De kosten van een audit worden door Praktijk gedragen.
5.6 Praktijk zal niet eerder aanvangen met een audit dan 14 (veertien) dagen na voorafgaande schriftelijke aankondiging. Indien datum en tijdstip van de audit HelloFysioApp niet gelegen komt, zal HelloFysioApp Praktijk daarvan op de hoogte stellen en een voorstel doen voor een vervangende datum.

Artikel 6. Vrijwaringen

6.1 HelloFysioApp vrijwaart Praktijk tegen elke rechtsvordering van derden, uit welke hoofde dan ook, in verband met de Persoonsgegevens of de uitvoering van de Bewerkersovereenkomst en/of Overeenkomst, tenzij HelloFysioApp bewijst alle technische en organisatorische maatregelen ter beveiliging van de Persoonsgegevens te hebben genomen zoals omschreven in deze Bewerkersovereenkomst.
6.2 Zijn de rechtsvorderingen van derden in verband met de Persoonsgegevens of de uitvoering van de Bewerkersovereenkomst en/of Overeenkomst het gevolg van opzet of grove nalatigheid gepleegd door HelloFysioApp dan is HelloFysioApp Praktijk in ieder geval vrijwaring verschuldigd.

Artikel 7. Geheimhouding

7.1 Op alle Persoonsgegevens die HelloFysioApp van Praktijk ontvangt en/of zelf verzamelt of dient te verzamelen met het doel deze te Verwerken overeenkomstig het in de Overeenkomst daartoe bepaalde, rust een geheimhoudingsplicht jegens derden.
7.2 HelloFysioApp zal deze informatie niet voor een ander doel gebruiken dan waarvoor zij deze heeft verkregen, zelfs niet wanneer deze in een zodanige vorm is gebracht zodat deze niet tot Praktijk of natuurlijke personen, zoals de Betrokkene, herleidbaar is.
7.3 De geheimhoudingsplicht is niet van toepassing voor zover Praktijk of de Betrokkene zelf uitdrukkelijk toestemming heeft gegeven of indien en voor zover er een wettelijke verplichting bestaat om informatie aan een derde te verstrekken.
7.4 Indien HelloFysioApp van de diensten van derden gebruik maakt, zorgt zij er onvoorwaardelijk voor dat deze derden dezelfde geheimhoudingsplicht als tussen Partijen is overeengekomen schriftelijk zal aanvaarden en deze geheimhoudingsplicht ook strikt zal naleven.

Artikel 8. Meldplicht

8.1 In het geval van een Lek, zal AuguSoft HelloFysioApp daarover informeren. HelloFysioApp beoordeelt of zij de Betrokkene(n) en/of de relevante toezichthouder(s) zal informeren of niet, en staat voor die keuze in.
8.2 De meldplicht behelst in ieder geval het melden van het feit dat er een Lek is geweest, alsmede:

- Wat de (vermeende) oorzaak is van het Lek;
- Wat is het (vooralsnog bekende en/of te verwachten) gevolg;
- Wat is de (voorgestelde) oplossing.

Artikel 9. Rechten van Betrokkene

In het geval dat Betrokkene een verzoek doet tot inzage, zoals bedoeld in art. 35 Wbp, of verbetering, aanvulling, wijziging of afscherming, zoals bedoeld in art. 36 Wbp, zullen Partijen het nodige doen dit verzoek in te willigen.

Artikel 10. Inschakelen van derden

10.1 Praktijk heeft HelloFysioApp toestemming gegeven om in het kader van de uitvoering van de Bewerkersovereenkomst derden in te schakelen.
10.2 HelloFysioApp is volledig verantwoordelijk voor deze derde en zal deze derde minstens dezelfde

verplichtingen ten opzichte van Praktijk opleggen als voor haarzelf uit deze Bewerkersovereenkomst voortvloeien.

Artikel 11. Aansprakelijkheid

11.1 HelloFysioApp is verantwoordelijk voor schade die het gevolg is van niet, niet tijdige of niet behoorlijke nakoming van de Bewerkersovereenkomst voor zover HelloFysioApp haar verplichtingen volgens de wet hierdoor niet nakomt.
11.2 Praktijk is aansprakelijk voor alle schade of nadeel die voortvloeit uit de niet nakoming van de Overeenkomst en/of deze Bewerkersovereenkomst en gegrond is op de betreffende wet- en regelgeving, tenzij de betreffende niet nakoming niet toerekenbaar is aan Praktijk.
11.3 Partijen zullen zich gedurende de Bewerkersovereenkomst adequaat verzekerd hebben en houden. De verzekeringsvoorwaarden hiertoe kunnen op verzoek worden ingezien.
11.4 Voor zover Partijen aansprakelijk zijn voor de schade of nadeel voortvloeiend uit de niet nakoming van deze Bewerkersovereenkomst of uit onrechtmatige daad of anderszins, dan is deze aansprakelijkheid beperkt tot het maximale bedrag waarvoor de bedrijfs- en/of beroepsaansprakelijkheidsverzekering schade uitkeert.

Artikel 12. Geschillenregeling

12.1 Op de Overeenkomst, alsmede op de hieruit voortvloeiende of hiermee samenhangende overeenkomsten en overige rechtshandelingen, is uitsluitend het Nederlandse recht van toepassing.
12.2 Alle geschillen, waaronder mede begrepen die slechts door één partij als zodanig worden beschouwd, worden beslecht door de bevoegde rechter in het arrondissement waar HelloFysioApp is gevestigd.

Artikel 13. Voorrang

Op de Bewerkersovereenkomst is de Overeenkomst van toepassing. In het geval van eventuele tegenstrijdigheid tussen de Overeenkomst en de Bewerkersovereenkomst, heeft het bepaalde in de Bewerkersovereenkomst voorrang.

Bijlage 1. Beveiligingsprotocol

Beveiligingsprotocol HelloFysioApp

Conceptversie: 1.0
Datum: 11 april 2014

Inhoud

1. Definities

De in dit document met een hoofdletter geschreven termen hebben de volgende definities:

Betrokkene	De persoon op wie de Persoonsgegevens betrekking hebben.
Bewerker	Degene die ten behoeve van de Verantwoordelijke Persoonsgegevens Verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Iedere dienstverlener die door de Praktijk wordt ingeschakeld en in opdracht van de Praktijk Persoonsgegevens Verwerkt, wordt als Bewerker beschouwd.
Datalek	Een ongeautoriseerde Verwerking of verlies van Persoonsgegevens. Veel voorkomende voorbeelden van Datalekken zijn: hackers die zich via het internet toegang verschaffen (bijvoorbeeld via malware, SQL injecties, cross-site scripting, etc.); het verlies van een laptop, smartphone, USB-stick of iets soortgelijks, documenten die naar het verkeerde adres zijn gestuurd, etc.
Persoonsgegeven	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon waarbij de Praktijk de Verantwoordelijke vormt.[1]
Risicoklasse I en II Persoonsgegevens	Persoonsgegevens waarvan de schade bij een Datalek gemiddeld of hoog wordt ingeschat. Tenzij de specifieke context waarin de gegevens zijn opgeslagen een ander risico meebrengt, kan hierbij worden gedacht aan: gezondheidsgegevens uit het Portal, gekoppeld aan identificerende gegevens (zoals naam en e-mailadres).
Risicoklasse III en IV Persoonsgegevens	Persoonsgegevens waarvan de schade bij een Datalek gering wordt ingeschat. Tenzij de specifieke context waarin de gegevens zijn opgeslagen een groter risico meebrengt, kan hierbij worden gedacht aan e-mailadressen en namen, voor zover deze niet kunnen worden gekoppeld aan de overige gegevens in het Portal. Ook kan worden gedacht aan gegevens die wellicht herleidbaar zouden kunnen zijn, maar waarvan herleiding moeilijk en feitelijk onwaarschijnlijk is.
Portal	Het HelloFysioApp Portal, een communicatieplatform en kennisbank voor de Praktijk, fysiotherapeuten en hun cliënten.
Praktijk	De fysiotherapiepraktijk die gebruik maakt van het Portal en aangemerkt kan worden als Verantwoordelijke.
Security Officer	De persoon die de eindverantwoordelijkheid heeft gekregen voor informatiebeveiliging.
Verantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt. De Praktijk wordt binnen dit document als Verantwoordelijke beschouwd.
Verwerken	Elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen,

[1] Een persoon is identificeerbaar “indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden”. Zie Kamerstukken II 1997-1998, 25 892, nr. 3, p. 47. Zie ook Advies 4/2007 over het begrip persoonsgegevens, goedgekeurd op 20 juni 2007 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf).

	vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.[2]
Wbp	Wet bescherming persoonsgegevens.

[2] Zie ook WP29, Advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en “verwerker”, goedgekeurd op 16 februari 2010 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf). Merk op dat de Wbp in plaats van de term “verwerker”, de term “bewerker” gebruikt, terwijl de betekenis inhoudelijk gelijk is.

2. Doel en achtergrond van dit document

Op grond van artikel 13 van de Wbp is de Praktijk verplicht tot het ten uitvoer leggen van passende technische en organisatorische maatregelen, om Persoonsgegevens te beveiligen tegen Datalekken. Volgens de wet moeten de maatregelen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de Verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen moeten er mede op zijn gericht onnodige verzameling en verdere Verwerking van Persoonsgegevens te voorkomen.

Op grond van artikel 14 Wbp is de Praktijk tevens verplicht om te zorgen dat personen die in opdracht van de Praktijk Persoonsgegevens Verwerken, zoals HelloFysioApp en AuguSoft, '(sub-)Bewerkers' genoemd, ook passende technische en organisatorische maatregelen ten uitvoer leggen.

Dit beveiligingsprotocol vormt een bijlage bij de Bewerkersovereenkomst die de Praktijk en HelloFysioApp (en eventuele sub-Bewerkers) hebben gesloten en bepaalt de technische en organisatorische maatregelen die HelloFysioApp als Bewerker en AuguSoft als sub-Bewerker van de Praktijk garandeert te implementeren.

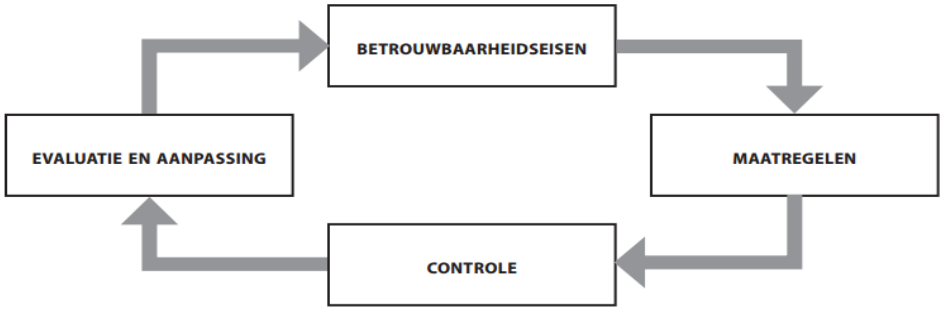
Dit beveiligingsprotocol bevat gevoelige informatie omtrent de beveiliging van het Portal en omgang met persoonsgegevens. Indien onbevoegden kennis nemen van deze informatie veroorzaakt dat een groot risico. Dit beveiligingsprotocol dient dan ook strikt vertrouwelijk behandeld te worden.

3. Totstandkoming, controle, evaluatie en aanpassing

Dit beveiligingsprotocol is opgesteld met behulp van de richtsnoeren[3] van het College Bescherming Persoonsgegevens (“CBP”; “Richtsnoeren”) en incorporeert diverse 'best-practices' en maatregelen uit commerciële en niet-commerciële standaarden omtrent informatiebeveiliging.[4]

Zoals in de Richtsnoeren van het CBP wordt benadrukt, is het noodzakelijk ervoor te zorgen dat de maatregelen met de tijd meegaan en passend *blijven*. Daarom dient dit document regelmatig te worden herzien. Het initiatief tot aanpassing zal in de praktijk door HelloFysioApp en AuguSoft worden genomen, waarbij deze partijen de Praktijk zullen informeren over de aanpassingen. Partijen zullen de aanpassingen vervolgens evalueren. HelloFysioApp kan, in samenspraak met de Praktijk, een aanpassing afkeuren indien deze volgens HelloFysioApp een vermindering van het beveiligingsniveau tot gevolg heeft. HelloFysioApp kan ook eigen aanpassingen voorstellen indien zij dat nodig acht.

Conform de Richtsnoeren gebeurt de totstandkoming, controle, evaluatie en aanpassing volgens de hieronder weergegeven voortdurende cyclus.



3.1. Herzieningsfrequentie

Mede gelet op de in hoofdstuk 4. weergegeven risico-analyse, dient dit document ten minste een keer per jaar te worden gecontroleerd, geëvalueerd en vernieuwd.

3.2. Audit en penetratietest

De Praktijk heeft het recht om conform artikel 5 van de Bewerkersovereenkomst door een derde te laten controleren of HelloFysioApp en de sub-Bewerkers de voorgeschreven maatregelen correct en volledig hebben geïmplementeerd.

De Praktijk en HelloFysioApp kunnen daarnaast in onderling overleg besluiten tot het doen uitvoeren van een penetratietest, door een ter zake deskundig bedrijf. Daarbij is het noodzakelijk dat toestemming wordt verkregen van alle andere relevante partijen die door de penetratietest geraakt zouden kunnen worden.

---

[3] http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[4] Waaronder ISO 27001-27002, NEN 7510, OWASP top 10, NCSC richtlijnen voor veilige webapplicaties, PCI DSS, etc.

4. Risico-analyse en betrouwbaarheidseisen

Hieronder volgt een omschrijving van de soorten Persoonsgegevens en Verwerkingen, de risico's en de hoogtes van de te verwachten schades bij verlies, aantasting en ongeautoriseerde toegang.

4.1. Aard van de Persoonsgegevens

HelloFysioApp ontwikkelt, beheert en onderhoudt in opdracht van de Praktijk het Portal.

Het Portal is een door HelloFysioApp geëxploiteerd en door AuguSoft ontwikkeld online platform welke het voor de Praktijk en daarbij aangesloten fysiotherapeuten mogelijk maakt om op afstand diensten te verlenen, te communiceren met cliënten en een kennisbank aan te leggen.

HelloFysioApp Verwerkt voor de hierboven omschreven doeleinden gegevens van de Praktijk, fysiotherapeuten en cliëntgegevens van de Praktijk.

Onder die gegevens bevinden zich het e-mailadres, voornaam, achternaam, geslacht, geboortedatum, telefoonnummer en foto's van fysiotherapeuten, de Praktijk en cliënten.
Uit de in de in het Portal ingevoerde gegevens kan ook de gezondheid van iemand worden afgeleid, wat een bijzonder persoonsgegeven vormt volgens de Wbp en waarop een strenger regime van toepassing is.[5]

IP-adressen van de gebruikers van het Portal worden gebruikt ter bestrijding van computerinbraak en logging.

4.2. Aard van de Verwerkingen

HelloFysioApp maakt gebruikt van computerprogramma's die door anderen, zoals AuguSoft, in licentie zijn gegeven. Ten behoeve van het Portal zijn verschillende veiligheidsmaatregelen in de broncode opgenomen, voor het beheren en beveiligen van de inhoud van de websites. Voor de database met gegevens wordt Microsoft Internet Information Services gebruikt en wordt open source software onder de naam MySQL en PHP gebruikt. Er bestaat documentatie en uitleg over security-aspecten met betrekking tot het gebruik van deze software, vanuit de ontwikkelaars van deze softwarepakketten.[6]
De servers vormen een cluster welke draait op VMWare ESX 4 platform. De servers zelf draaien op Microsoft Windows 2008 Server R2 waarbij updates automatisch worden geïnstalleerd.

HelloFysioApp is verantwoordelijk voor de hosting van het Portal. De hosting koopt HelloFysioApp in bij AuguSoft. AuguSoft beheert in opdracht van HelloFysioApp een Private Virtual Server bij DCG, een ISO 27001 gecertificeerd datacenter in Amsterdam, en waarborgt de passende technische en organisatorische beveiligingsmaatregelen. AuguSoft is exclusief belast met het dagelijkse beheer en garandeert een uptime van 99,9%.

4.3. Risico's

Begin 2012 heeft het Nationaal Cyber Security Centrum (NCSC)[7] beveiligingsrichtlijnen ten behoeve van webapplicaties opgesteld. In deze richtlijnen worden risico's als volgt gedefinieerd:

---

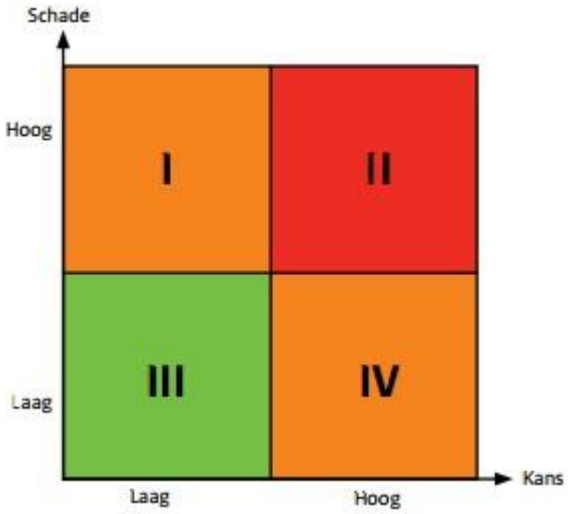
[5] Zie art. 16 en 21 Wbp.

[6] Voor MySQL: http://dev.mysql.com/doc/mysql-security-excerpt/5.1/en/index.html. Voor PHP: http://www.php.net/manual/en/security.php

[7] Het Nationaal Cyber Security Centrum (NCSC) bestaat sinds 1 januari 2012. Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein en daarmee aan een veilige, open en

Risico is het product van de kans op optreden van een ongewenste gebeurtenis en de mogelijke schade als gevolg van deze ongewenste gebeurtenis (risico = kans x schade)[8]

In diezelfde richtlijn worden de risico's in kaart gebracht door middel van een matrix waarbij de risicocategorieën gedefinieerd worden. Waarbij categorie I en IV een gemiddeld risico vormen, zorgt categorie II voor een hoog risico en categorie III voor een laag risico.
Deze categorieën zullen in dit beveiligingsprotocol in hoofdlijnen aangehouden worden.
Logischerwijs zullen risico's die vallen in de eerste en tweede categorie meer prioriteit hebben dan risico's die in de derde en vierde categorie vallen, immers risico's die veel schade tot gevolg hebben verdienen de meeste aandacht.



Ongeautoriseerde toegang

De risico's bevinden zich met name op het vlak van het lekken van de in de Portal besproken gegevens tussen cliënten en fysiotherapeuten of de Praktijk. Het is hoogstwaarschijnlijk dat er in de relatie tussen fysiotherapeuten en cliënten gesproken zal worden over gezondheid. Deze gesprekken vormen in combinatie met de overige Persoonsgegevens, zoals de naam van de cliënt, een waardevol doelwit voor hackers of andere kwaadwillende. De schade, zowel financieel als reputatieschade, zal voor de Praktijk, maar ook voor HelloFysioApp en AuguSoft desastreus zijn. Het verlies van dergelijke Persoonsgegevens kan op basis van bovenstaande matrix in categorie I of II ingedeeld worden.

Wanneer de beveiliging tekort zou schieten, zou dat ook strijd betekenen met een wettelijke norm, namelijk artikel 13 en/of 14 Wbp. Dat vormt een grondslag voor aansprakelijkheid, conform art. 6:162 BW. Verder is er een Europese Privacyverordening op komst, waarbij het huidige concept aanzienlijke en afschrikwekkende boetebevoegdheden toebedeelt aan privacy-autoriteiten.[9]

Onbedoelde vernietiging of aantasting

De schade bij onbedoelde vernietiging of aantasting van bestanden, zonder dat onbevoegden deze in kunnen zien, wordt lager ingeschat en is in te delen in categorie III of IV. De consequenties van onbedoelde vernietiging of aantasting lijken beperkt tot het opnieuw aanleggen van een digitaal dossier of het opnieuw aanmaken van een account in het Portal. Door de dagelijkse backup die AuguSoft beschikbaar stelt zal de schade beperkt zijn.

---

stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief. Bron: https://www.ncsc.nl/organisatie

[8] Bron: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[9] De versie die op 21 oktober 2013 door het Europees Parlement is aangenomen, bepaalt boetes tot 100 miljoen of 5% van de wereldwijde omzet.

Het niet beschikbaar zijn van het Portal

Indien het Portal vanwege onderhoud of een storing tijdelijk niet beschikbaar is, levert dat waarschijnlijk eerder enig ongemak op dan werkelijke schade voor Betrokkenen. Dit risico is in te schalen in de categorieën III en IV. Het ongemak dat de Praktijk of fysiotherapeuten ondervinden wegens het niet beschikbaar zijn van het Portal wordt ondervangen door boetebepalingen in het hostingcontract gesloten tussen HelloFysioApp en AuguSoft.

Geschatte schades

De werkelijk te verwachten totale schade is vooraf moeilijk in een getal uit te drukken, maar bij een Datalek van enige omvang, waarbij van een aanzienlijk aantal Betrokkenen het complete ingevulde (gezondheids) dossier inclusief identificerende gegevens (zoals naam en e-mailadres) openbaar zouden zijn, zou de schade kunnen oplopen tot enkele honderdduizenden euro's.

4.4. Betrouwbaarheidseisen

De betrouwbaarheidseisen zien om bovenstaande redenen met name op het goed afgesloten zijn van de Persoonsgegevens voor onbevoegden, in het bijzonder de Risicoklasse I en II Persoonsgegevens (waaronder gegevens over de gezondheid van Betrokkenen). Alleen de daartoe gemachtigde personen binnen de Praktijk, fysiotherapeuten, Betrokkenen, de daartoe gemachtigde personen binnen HelloFysioApp en de daartoe gemachtigde personen binnen AuguSoft, hebben rechtstreekse toegang tot de volledige databases met alle gegevens die via het Portal worden verzameld en verder verwerkt. De Praktijk, fysiotherapeuten en Betrokkenen hebben alleen toegang tot de voor hen relevante Persoonsgegevens. HelloFysioApp en AuguSoft hebben toegang tot de gehele database van het Portal.

5. Organisatorische beveiligingsmaatregelen

5.1. Algemene organisatorische maatregelen

De Security Officer is (eind)verantwoordelijk voor informatiebeveiliging en ziet erop toe dat de minimale technische en organisatorische beveiligingsmaatregelen worden nageleefd en dat dit concreet kan worden geverifieerd. Onderstaand volgt een overzicht van de overeengekomen beveiligingsmaatregelen.

5.2. Preventieve maatregelen[10]

5.2.1. In de Gebruiksvoorwaarden voor het Portal is opgenomen dat gebruikers zelf zorg dienen te betrachten met betrekking tot bescherming en geheimhouding van hun inloggegevens.

5.2.2. Met AuguSoft zijn afspraken gemaakt zodat de medewerkers van deze partij zelf geen toegang zullen hebben tot de gegevens op de servers, behalve met uitdrukkelijke toestemming van de Praktijk en/of HelloFysioApp.

5.2.3. Alleen personen die vanuit hun functie een legitieme noodzaak tot Verwerking van Persoonsgegevens hebben, zullen de middelen en gegevens ontvangen die vereist zijn om (via fysieke of digitale weg) toegang te verkrijgen tot de Persoonsgegevens.

5.2.4. Alle medewerkers die Persoonsgegevens Verwerken, worden deugdelijk geïnformeerd over welke vormen van Verwerking zijn toegestaan en welke niet. De bedoelde medewerkers hebben in elk geval dit beveiligingsprotocol ontvangen en gelezen.

5.2.5. Alle medewerkers van AuguSoft die toegang hebben tot Persoonsgegevens hebben een geheimhoudingsverklaring getekend, waarin de medewerker verklaart de Persoonsgegevens uitsluitend te zullen Verwerken volgens de instructies van de Praktijk of van de Bewerker, deze niet aan onbevoegde derden te verstrekken of openbaar maken en te allen tijde de geldende protocollen voor veilige Verwerking van Persoonsgegevens, waaronder dit beveiligingsprotocol, zal naleven.

5.2.6. Van alle medewerkers van fysiotherapiepraktijken die toegang hebben tot Risicoklasse I en II Persoonsgegevens is een BIG registratie aanwezig.

5.2.7. Gegevens waarmee toegang kan worden verkregen tot Persoonsgegevens, zoals gebruikersnamen, wachtwoorden en tokens of smartcards, worden zorgvuldig bewaard door de persoon aan wie ze zijn verstrekt. Er worden bijvoorbeeld geen post-it's met dergelijke gegevens op schermen geplaatst als niet tot Verwerking bevoegd personeel die post-it's ook kan zien en tokens, smartcards en sleutels zijn niet vrij toegankelijk maar worden opgeborgen in (bij voorkeur met slot en grendel) afgesloten ruimtes.

5.2.8. Personen die een persoonlijk belang, anders dan zuiver het belang van het uitoefenen van de functie, hebben bij bepaalde Persoonsgegevens die in de systemen (servers/applicaties) worden Verwerkt, krijgen geen toegang tot de systemen, tenzij de betreffende Persoonsgegevens dusdanig zijn afgeschermd dat het onmogelijk is voor die personen om

[10] Primair gericht op het voorkomen van Datalekken. De onderverdeling van maatregelen in preventieve, detectieve, mitigerende en correctieve maatregelen, is enkel bedoeld als nuttige indicatie en dient niet te strikt te worden geïnterpreteerd.

toegang tot de Persoonsgegevens te krijgen, zelfs als zij wel toegang hebben tot de systemen.[11]

5.3. Detectieve maatregelen[12]

5.3.1. De Security Officer controleert periodiek steekproefsgewijs (en zo discreet mogelijk, met inachtneming van een redelijk niveau van privacy voor de medewerkers) of medewerkers zich de van hen verwachte maatregelen nemen en niet zelf ongeautoriseerde Verwerkingen uitvoeren of Datalekken veroorzaken.

5.3.2. Medewerkers die zelf een (mogelijk) Datalek hebben veroorzaakt door het nalaten de juiste maatregelen te treffen en die dat eerlijk en tijdig melden aan de leidinggevende en/of Security Officer, krijgen lichtere sancties.

5.4. Mitigerende en herstelmaatregelen[13]

5.4.1. Zodra iemand in de organisatie weet van een Datalek met mogelijk schadelijke gevolgen, dient deze de Security Officer in te lichten.

5.4.2. De Security Officer ziet erop toe dat indien nodig de juiste personen buiten de organisatie tijdig worden geïnformeerd over het Datalek. In elk geval dient de projectleider bij HelloFysioApp te worden geïnformeerd.

5.4.3. De Security Officer voert de regie en kent waar nodig taken en verantwoordelijkheden toe aan ander personeel om schade als gevolg van een Datalek zo veel en zo snel mogelijk te beperken en soortgelijke Datalekken in de toekomst te voorkomen.

5.5. Correctieve maatregelen[14]

5.5.1. Het arbeidscontract, arbeidsreglement en/of geheimhoudingsverklaring bevat sancties voor het geval van schending van de geheimhoudingsplicht of het niet naleven van beveiligingsprotocollen. De sancties zijn proportioneel tot de ernst van de overtreding.

5.5.2. Periodiek worden besprekingen gehouden met relevant personeel om de effectiviteit en proportionaliteit van genomen maatregelen te evalueren en indien zich een Datalek heeft voorgedaan, daar lessen uit te trekken en de maatregelen aan te scherpen.

---

[11] Het kan niet volledig worden gegarandeerd dat iemand toegang krijgt tot vertrouwelijke gegevens van iemand die deze persoon kent. Deze gegevens dienen strikt vertrouwelijk te worden behandeld en mogen op geen enkele wijze ten nadele van de betrokken persoon worden gebruikt of ingezet.

[12] Primair gericht op het weten dat er een Datalek heeft plaatsgevonden.

[13] Primair gericht op het beperken van negatieve gevolgen van Datalekken.

[14] Primair gericht op het repareren van tekortkomingen in de beveiliging die tot Datalekken hebben geleid of daar waarschijnlijk toe zouden kunnen leiden.

6. Technische beveiligingsmaatregelen

6.1. Algemene technische maatregelen

6.1.1. De Praktijk en/of HelloFysioApp dienen kennis te nemen van alle beveiligingsmaatregelen die door de ontwikkelaars van de gebruikte (open source) softwarepakketten worden aanbevolen ten behoeve van de informatieveiligheid. Voor iedere aanbevolen maatregel geldt het 'pas-toe-of-leg-uit' principe. Elke maatregel moet in beginsel worden doorgevoerd en alleen als er een zwaarder wegende reden is om dat niet te doen, kan dat achterwege blijven.

6.2. Preventieve maatregelen

6.2.1. De volgende beveiligingsmaatregelen zijn van toepassing voor alle servers (computers) die bereikbaar zijn vanaf het internet en Persoonsgegevens Verwerken.

6.2.2. Ruimtes met servers waarmee Persoonsgegevens worden Verwerkt, zijn alleen te betreden door bevoegd personeel. Bij servers waarop Risicoklasse I en II Persoonsgegevens worden Verwerkt, is de ruimte voorzien van een automatisch sluitende deur, die alleen te openen is met de juiste fysieke, magnetische of biometrische sleutel.

6.2.3. Remote toegang tot de servers met Risicoklasse I en II Persoonsgegevens wordt beveiligd met veilige wachtwoorden en/of tokens. De software waarmee de remote toegang plaatsvindt, bevat maatregelen tegen 'brute force' -aanvallen, zoals het beperken van het aantal mogelijke inlogpogingen per tijdseenheid en het 'blacklisten' van IP-adressen waarmee excessieve hoeveelheden inlogpogingen worden gedaan.

6.2.4. Wachtwoorden die worden gebruikt ter authenticatie van personen die tot Verwerking van Risicoklasse I en II Persoonsgegevens bevoegd zijn, zijn voldoende lang en niet gemakkelijk te raden. Daarbij wordt aangesloten bij gangbare richtlijnen over veilige wachtwoorden, zoals bijvoorbeeld verschaft door Microsoft via http://www.microsoft.com/nl-nl/security/online-privacy/passwords-create.aspx.

6.2.5. De software op de servers wordt zorgvuldig up-to-date gehouden via een degelijk patch management proces.[15]

6.2.6. Als de server wordt gebruikt voor Verwerking van Risicoklasse I en II Persoonsgegevens, wordt deze alleen ingezet voor het uitvoeren van de bedoelde Verwerkingen en niet voor andere taken. Een (al dan niet virtuele) server waarop de databases met (gezondheids) dossiers van Betrokkenen en bijbehorende rapportages en analyses staan opgeslagen, wordt bijvoorbeeld niet daarnaast gebruikt om ook nog een mailserver te draaien of een website te hosten, anders dan het Portal en mailservers horende bij het Portal.

6.2.7. De diensten die worden aangeboden door de server moeten zijn voorzien van authenticatie, zodat alleen geautoriseerde gebruikers toegang hebben tot de diensten.

6.2.8. Alle toegang tot Risicoklasse I en II Persoonsgegevens dient te worden vastgelegd (gelogd). Bij het vastleggen van de toegang dient tenminste de datum, tijd (inclusief tijdzone), de geautoriseerde gebruiker en de omschrijving van de verschafte toegang te worden vastgelegd.

[15] Zoals opgenomen in artikel 2.3 van het hostingcontract.

6.2.9. Persoonsgegevens worden zoveel als mogelijk is geanonimiseerd Verwerkt en niet langer opgeslagen dan noodzakelijk is.

6.3. Detectieve maatregelen

6.3.1. Op de server is een up-to-date virusscanner geïnstalleerd van een algemeen als betrouwbaar beschouwd merk.

6.3.2. Er wordt gebruik gemaakt van deugdelijk geconfigureerde firewalls.

6.3.3. Servers waarop Risicoklasse I en II Persoonsgegevens worden Verwerkt, zijn voorzien van software die erop is gericht om aanvallen te detecteren en voorkomen.

6.4. Mitigerende en herstelmaatregelen

6.4.1. Er is een procedure aanwezig voor het met behulp van backups herstellen van verloren Persoonsgegevens (restore-procedure). De restore-procedure wordt regelmatig getest, en zo ingericht dat de periode tussen het moment waarop een backup is gemaakt en deze is gebruikt voor herstel, nooit meer dan één dag bedraagt.

6.5. Correctieve maatregelen

6.5.1. Indien een Datalek zich heeft voorgedaan, wordt onder leiding van de Security Officer onderzocht wat de belangrijkste technische oorzaken van het Datalek zijn geweest. De technische maatregelen worden zodanig aangepast dat de geïdentificeerde technische oorzaken niet nogmaals tot een Datalek kunnen leiden.

7. Complete lijst met concrete beveiligingsmaatregelen

De beveiliging is op te splitsen in een aantal onderdelen. AuguSoft heeft de volgende onderverdeling gemaakt:

1. Fysieke beveiliging van de servers
2. Elektronische beveiliging van de server
3. Softwarematige beveiliging
4. Interne veiligheidsmaatregelen van AuguSoft
5. Gebruikersbeheer
6. Backup locaties

7.1. Fysieke beveiliging van het serverpark

Alle servers staan opgesteld in een 24uur per dag beveiligde locatie. De beveiliging bestaat o.a. uit toegangspassen en bemande videobewaking. Toegang is niet mogelijk zonder goedkeuring, identificatie en controle. De servers staan in een rack met een code slot. Toegang wordt uitsluitend verleend aan medewerkers van AuguSoft en alleen indien hier noodzaak voor is.

7.2. Elektronische beveiliging van het serverpark

Van alles servers in het AuguSoft netwerk is de bios beveiligd met een wachtwoord. Er kan niet van een ander medium opgestart worden dan van de harde schijf. De servers vormen samen een cluster welke uitsluitend beheerd wordt door medewerkers van AuguSoft. Het cluster draait op het VMWare ESX 4 platform. Toegang tot het cluster is uitsluitend mogelijk middels een beveiligde verbinding.

7.3. Beveiliging server

De server gebruikt Microsoft Windows 2008 Server R2 als besturingssysteem. Updates worden automatisch toegepast.
De externe toegang tot de server is alleen mogelijk over de TCP poorten 21, 25, 53, 80, 110 en 443. Enkele andere poorten zijn uitsluitend toegankelijk vanaf AuguSoft beheer locaties.
Het aantal Windows gebruikers op de server is tot een minimum beperkt en rechten zijn alleen toegekend aan de gebruikers waarvoor dit strikt noodzakelijk is. Voor alle gebruikers is een ‘moeilijk’ wachtwoord ingesteld.
Het Portal gebruikt een Internet Information Services(IIS) 7, MySQL 5.1 en PHP 5 combinatie met de meeste recente versies.

7.4. Beveiliging broncode

In de broncode van het Portal zijn een aantal veiligheidsconstructies in acht genomen.
Dit zijn algemene uitgangspunten waarop alle door AuguSoft geleverde code wordt gecontroleerd:

- Alle input wordt op het juiste type gecontroleerd. Foutieve, onveilige invoer wordt daarmee afgevangen.
- Fouten worden niet getoond aan de gebruiker.
- Er wordt overal gecontroleerd op SQL injectie zowel bij het wegschrijven als bij het opvragen van data.
- Session Hijacking wordt getracht te voorkomen door extra controles buiten de SESSIONID.
- De SESSIONID wordt opnieuw gegenereerd na het inloggen.

- Het gebruik van SSL verbindingen wordt geforceerd bij de niet publieke onderdelen van het Portal.
- Bij het optreden van fouten wordt direct een foutrapportage gemaakt en een melding gestuurd aan AuguSoft (per email). Hackpogingen worden daar snel mee gevonden.
- Het gebruik van het Portal wordt uitgebreid gelogd. Oneigenlijk gebruik van gebruikers kan hiermee worden opgespoord.
- Het is voor gebruikers technisch niet mogelijk om gegevens te bekijken waar zij geen toegang toe mogen hebben. Een strikte scheiding tussen gebruikersgegevens wordt gewaarborgd.

7.5. Organisatorische maatregelen binnen AuguSoft

- Wachtwoorden om toegang te verkrijgen tot de servers worden uitsluitend vertrekt aan medewerkers indien hier noodzaak voor is.
- Alle werknemers hebben een geheimhoudingsclausule ondertekend voor het geval zij in aanraking komen met al dan niet gevoelige informatie.
- Medewerkers hebben alleen toegang tot een deel van de database(kopie) indien hier noodzaak voor bestaat.
- Bij het gebruik van de database voor ontwikkeling worden Persoonsgegevens geanonimiseerd.
- Bij het gebruik van de database voor ontwikkeling worden alle gegevens met betrekking tot beveiliging gewist.
- Na gebruik voor ontwikkeling wordt de lokale kopie weer verwijderd.

7.6. Gebruikersbeheer

Een encryptie algoritme draagt er zorg voor dat wachtwoorden van gebruikers niet te achterhalen, kraken of raden zijn.

7.7. Backup locaties

Er worden backups opgeslagen op het serverpark van AuguSoft. Deze zijn uitsluitend toegankelijk voor herstelwerkzaamheden en kunnen indien noodzakelijk geanonimiseerd gebruikt worden voor ontwikkelingsdoeleinden.

7.8. Monitoring / Beveiligingsmeldingen

Bij elke incident in een aanroep wordt er automatisch een gedetailleerde email naar AuguSoft gestuurd. Dit bericht bevat alle relevantie informatie met betrekking tot deze fout. Hierdoor kunnen hackpogingen op een makkelijke manier worden opgespoord. Ook hackpogingen zijn op deze manier direct zichtbaar.

7.9. Beveiliging broncode

AuguSoft doet er alles aan om het Portal zo veilig mogelijk te maken. Onderstaande kenmerken geven een indicatie van de eisen die worden gesteld bij de ontwikkeling van onderdelen.

Eenmalige authenticatie:	De authenticatie vindt plaats via een beveiligde verbinding. Na het inloggen vind er bij elke aanroep een controle plaats.
1-weg wachtwoord encryptie:	Wachtwoorden zijn niet terug herleidbaar uit database of andere bronnen.
Beveiliging op module niveau:	De beveiliging op module niveau zorgt voor een goede scheiding van functionaliteiten per gebruikerstype.
Beveiliging op IP niveau:	Indien noodzakelijk kunnen bepaalde functionaliteiten worden beperkt middels IP-adressen.
Beveiliging op dataniveau:	Indien mogelijk wordt er ook op dataniveau bepaald wie er toegang heeft tot bepaalde informatie.
Instelbaar maximum aantal inlog pogingen:	Door monitoring op de voordeur kunnen pogingen tot misbruik voortijdig worden gedetecteerd.
Foutrapporten:	Er worden geen risicovolle foutmeldingen aan de gebruiker getoond.
Hackreports:	Pogingen door hackers kunnen meestal worden gedetecteerd. Hiervan wordt direct melding gemaakt aan de beheerder en een automatische blokkade kan worden ingesteld.
Schaduwdatabase:	Alle wijzigingen die in het Portal plaatsvinden worden geregistreerd op naam. Hierdoor kan het verlies van data worden beperkt en is altijd terug te zoeken wie er een wijziging heeft doorgevoerd.
Automatisch uitloggen:	Door het opgeven van een verlooptijd wordt de gebruiker automatisch afgemeld na een periode van inactiviteit.
Toegang via SSL:	Er kan op broncodeniveau worden afgedwongen dat de portal alleen via SSL mag worden benaderd.
Registratie van gebruikers:	Het gebruik van het Portal en pogingen om in te loggen worden geregistreerd.