Versienummer	1.2
Datum vastgesteld	20 mei 2019
Autorisator	B. Reiss
Beheerder	M. Friso – van Peer
Evaluatiedatum	Mei 2020

Privacyreglement patiënten

Stichting Huisartsenpost Amstelland

Inhoud

1. Doel

Het privacyreglement van Stichting Huisartsenpost Amstelland (SHA) geeft een overkoepelend beeld over de privacy en informatiebeveiliging van persoonsgegevens en is bestemd voor alle patiënten van de SHA. Het reglement omschrijft de uitgangspunten met betrekking tot het gebruik van persoonsgegevens en omschrijft de organisatorische maatregelen op het gebied van privacybescherming.

2. Begrippenlijst

AP = Autoriteit Persoonsgegevens, de toezichthouder voor het toezicht op het verwerken van persoonsgegevens
AVG= Algemene Verordening Gegevensbescherming
BoZ = Brancheorganisaties Zorg
BSN = Burger Service Nummer
DPIA = Data Protection Impact Analyse
FG = Functionaris Gegevensbescherming
IGJ = Inspectie voor de Gezondheidszorg en Jeugd
NTS = Nederlandse Triage Standaard
SHA = Stichting Huisartsenpost Amstelland
UZI = Unieke Zorgverlener Identificatie
WGBO = Wet op de Geneeskundige Behandelovereenkomst
Wet BIG = Wet Beroepen Individuele Gezondheidszorg
Wkkgz = Wet kwaliteit, klachten en geschillen zorg
ZHA = Ziekenhuis Amstelland

3. Toepassingsbereik

Het privacyreglement heeft betrekking op:

- Alle persoonsgegevens die verwerkt worden door de SHA, zowel op papier als digitaal.
- Patiënteninformatie die ontleend kan worden aan de gegevensverzamelingen van de SHA of persoonsgegevensverzamelingen van derden die de SHA in haar beheer heeft.
- De (geautomatiseerde) informatiesystemen van de SHA.

Het reglement is bestemd voor alle patiënten van de SHA.

4. Uitgangspunten

De uitgangspunten in dit reglement zijn gebaseerd op wettelijke vereisten. Per 25 mei beoogt Stichting Huisartsenpost Amstelland te voldoen aan de Algemene Verordening Gegevensbescherming (AVG), een Europese verordening betreffende bescherming van persoonsgegevens. De SHA heeft daarnaast te maken met andere regelgeving, zoals de Wet op de Geneeskundige Behandelovereenkomst (WGBO); Geneesmiddelenwet; Wet Beroepen Individuele Gezondheidszorg (wet BIG) en de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Naast de wettelijke vereisten heeft de SHA als uitgangspunt dat de fysieke beveiliging van de computers en gebouwen van de SHA zodanig is ingericht dat de vertrouwelijkheid, integriteit en continuïteit van de gegevens en gegevensverwerking gewaarborgd zijn. In hoofdstuk 9 en verder wordt dit informatiebeveiligingsbeleid verder uitgewerkt.

5. Verwerking van persoonsgegevens

5.1 Inleiding

De SHA heeft altijd een grondslag nodig voor de verwerking van persoonsgegevens. Dit betekent dat de SHA altijd een geldige reden moet hebben om persoonsgegevens te gebruiken. Indien er geen geldige grondslag bestaat, mag de SHA de persoonsgegevens niet verwerken. De wet geeft zes grondslagen voor verwerking van persoonsgegevens. Gegevensverwerking is noodzakelijk voor de behartiging van gerechtvaardigd belang, noodzakelijk voor de uitoefening van een publiekrechtelijke taak, is van levensbelang voor de betrokkene, is noodzakelijk voor een wettelijke verplichting, is noodzakelijk voor de uitvoering van een overeenkomst, óf de betrokkene geeft toestemming voor de verwerking.

5.2 Wat zijn (bijzondere) persoonsgegevens?

Alle informatie over een geïdentificeerde of identificeerbaar natuurlijk persoon. Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd. Bijvoorbeeld aan de hand van een naam, een identificatienummer, of elementen die kenmerkend zijn voor de fysieke of genetische identiteit van die persoon. Bijzondere persoonsgegevens zijn gegevens over ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, gegevens over lidmaatschap van een vakbond en verwerking van genetische en biometrische gegevens en gegevens over gezondheid. Tevens heeft de Autoriteit Persoonsgegevens bepaald dat het Burger Service Nummer (BSN) als een bijzonder persoonsgegeven moet worden verwerkt. De verwerking van bijzondere persoonsgegevens is aan strikte regels onderworpen. Binnen de SHA worden bijzondere persoonsgegevens alleen verwerkt indien dit wettelijk is toegestaan of indien de betrokkene toestemming geeft voor de verwerking en indien voldoende technische en organisatorische waarborgen in acht zijn genomen.

5.3 Welke persoonsgegevens verwerkt de SHA?

De SHA verwerkt administratieve, verzekerings- en medische gegevens van patiënten. Dit vindt plaats om acute huisartsgeneeskundige zorg te kunnen leveren in de avonden (17.00 uur – 23.00 uur), de nachten (23.00 uur – 8.00 uur), de weekenden en op officieel erkende feestdagen. En om de declaratie van geleverde prestaties aan de ziektekostenverzekeraar van de patiënt door te berekenen. Naast deze doelen voor verwerking van persoonsgegevens, vindt er ook verwerking van persoonsgegevens plaats voor zorgonderzoek en verbetering ter kwaliteitsbevordering van de SHA.

5.4 Verwerkingsregister

Voor iedere verwerking moet vooraf worden vastgesteld waarvoor de persoonsgegevens worden gebruikt. Deze doeleinden moeten heel concreet worden beschreven. Een omschrijving van alle verwerkingen zijn opgenomen in het verwerkingsregister van de SHA. Hierin staat het doel van de activiteit, de betrokkenen, ontvangers, categorie van gegevens, bewaartermijnen, additionele maatregelen, grondslag van de verwerking, de verwerker en of er een verwerkersovereenkomst is afgesloten. Dit verwerkingsregister wordt jaarlijks, of bij het uitvoeren van een nieuwe verwerking bijgewerkt door de kwaliteitsmedewerker en daarna geëvalueerd door de functionaris gegevensbescherming. Bij een nieuwe verwerking wordt tevens de afweging gemaakt of er een data protection impact analyse gedaan moet worden. Dit is een onderzoek waarbij de nieuwe verwerking onderzocht wordt op privacyrisico's.

5.5 Verwerkersovereenkomst

De SHA sluit een verwerkersovereenkomst met partijen die persoonsgegevens verwerken. De overeenkomst is gebaseerd op het format van de Brancheorganisaties Zorg (BoZ) en wordt indien

noodzakelijk tevens juridisch getoetst. Dit doet zij opdat partijen die persoonsgegevens verwerken voor de SHA dat net zo zorgvuldig doen als de SHA zelf.

5.6 Bewaartermijnen

Als uitgangspunt hanteert de SHA dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is voor het doel waarvoor zij verzameld zijn. Het hanteren van bewaartermijnen en het tijdig vernietigen van gegevens na afloop van deze termijnen, zorgt voor een verkleining van privacy risico's voor betrokkenen. De SHA heeft haar bewaartermijnen voor verwerkingen vastgesteld en juridisch laten toetsen

De procedure bewaartermijnen geeft in grote lijnen aan hoe de SHA omgaat met bewaartermijnen en welke afspraken er zijn gemaakt. Dit betreft de bewaartermijnen van digitale informatie ten aanzien van patiënten. Hierbij wordt uitgegaan van relevante wetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), het Burgerlijk Wetboek en de Wet op de geneeskundige behandelingsovereenkomst (WBGO). In het verwerkingsregister van de SHA staan de bewaartermijnen beschreven voor de diverse categorieën van persoonsgegevens. De vernietiging van persoonsgegevens na afloop van de bewaartermijn zoals opgenomen in het verwerkingsregister wordt nageleefd, en jaarlijks gecontroleerd en geëvalueerd bij de revisie van het verwerkingsregister.

6. Functionaris gegevensbescherming

De directie van de SHA heeft een functionaris gegevensbescherming (FG) aangesteld om naleving van de AVG te waarborgen en beleid rondom privacy en informatiebeveiliging te waarborgen, conform Artikel 37-AVG.

De FG is de privacy toezichthouder binnen de SHA. Deze functionaris voldoet aan de wettelijke kwalificaties, oefent haar taken uit in onafhankelijkheid en handelt volgens de gedragsregels FG. Ze informeert en adviseert de directie over maatregelen die genomen moeten worden om de gegevensbescherming op de SHA te optimaliseren en te laten voldoen aan de huidige wet en regelgeving. Ze geeft advies over het melden van een datalek bij de Autoriteit Persoonsgegevens (AP). Tevens kan ze fungeren als contactpersoon richting de AP.

Om haar taken goed uit te kunnen voeren wordt de FG goed gepositioneerd binnen de SHA, conform Artikel 38-AVG. Zij wordt tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Ze heeft een nauwe samenwerking met de kwaliteitsmedewerker van de SHA. Aan de mening van de FG wordt passende waarde gehecht, bij geschillen wordt vastgelegd waarom het advies van de FG niet gevolgd is.

De SHA ondersteunt de FG bij de uitvoering van haar taken en biedt haar de mogelijkheid om haar rol onafhankelijk te kunnen vervullen. De SHA geeft de FG geen instructies, bijvoorbeeld met het oog op het beoogde resultaat van een onderzoek, hoe een klacht dient te worden afgehandeld, of omtrent het betrekken van de AP.

7. Rolverdeling en verantwoordelijkheden

De primaire verantwoordelijkheid voor de omgang met persoonsgegevens ligt bij de medewerkers en werknemers zelf. Zij zijn op de hoogte van de gedragsregels op de SHA (zie voor een toelichting hoofdstuk 8).

De SHA heeft een functionaris gegevensbescherming aangesteld die een adviserende en toezichthoudende taak heeft met betrekking tot privacy gerelateerde onderwerpen. De functionaris gegevensbescherming (FG) rapporteert rechtstreeks aan de directeur en werkt nauw samen met de

kwaliteitsmedewerker (privacy officer). De FG en de kwaliteitsmedewerker (privacy officer) vormen de vraagbaak voor de organisatie en ondersteunen met verdergaande bewustwording rondom de privacywetgeving. Het SHA-bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de SHA. Handhaving, implementatie en evaluatie van dit beleid is gedelegeerd aan de SHA-directeur. De Autoriteit persoonsgegevens ziet toe op de naleving van de Algemene Verordening Gegevensbescherming. De Inspectie voor de Gezondheidszorg en Jeugd (IGJ) richt zich op het naleven van regels rondom verantwoorde zorg.

Taken en verantwoordelijkheden directeur:

- Het vaststellen en wijzigen van het privacy en informatiebeveiligingsbeleid.
- Het toekennen van rollen en verantwoordelijkheden conform autorisatieschema's (zie bijlage 1)
- Het signaleren van belangrijke wijzigingen in bedreigingen waaraan de bedrijfsinformatie wordt blootgesteld.
- Signaleren van belangrijke wijzigingen in wet en regelgeving omtrent informatiebeveiliging en privacy.
- Het bespreken van en toezicht houden op beveiligingsincidenten.
- Het goedkeuren van maatregelen ter verbetering van de privacy.
- Het goedkeuren van acties met betrekking tot het bewustwordingsproces van informatiebeveiliging en privacy onder de medewerkers en werknemers.
- Het implementeren van het privacy en informatiebeveiligingsbeleid in de organisatie.
- Het uitvoeren van een 3-jaarlijkse risicobeoordeling.
- Het nemen van maatregelen ter verbetering van de informatiebeveiliging.
- O.b.v. incidenten monitoren of het privacy en informatiebeveiligingsbeleid wordt nageleefd.

De directeur heeft de volgende taken gedelegeerd aan de kwaliteitsmedewerker (privacy officer):

- Signaleren van belangrijke wijzigingen in wet en regelgeving omtrent informatiebeveiliging en privacy.
- De jaarlijkse revisie en toetsing van het privacy en informatiebeveiligingsbeleid aan de huidige normen, wet- en regelgeving.

De directeur heeft de volgende taken gedelegeerd aan de functionaris gegevensbescherming (FG):

- De FG informeert en adviseert de SHA over haar verplichtingen op grond van de AVG.
- De FG ziet toe op de naleving van de AVG en het interne beveiligingsbeleid van de SHA.
- De FG adviseert op verzoek over de risicobeoordeling en ziet toe op de uitvoering daarvan.
- De FG werkt samen met en treedt op als contactpunt voor de Autoriteit Persoonsgegevens.
- De FG rapporteert ieder kwartaal over de uitvoering van haar taken aan de directeur van de SHA.

8. Privacy werknemers en medewerkers van de SHA

De SHA zorgt ervoor dat de werknemers en medewerkers in haar organisatie op de hoogte zijn van de privacyregels. Zij worden op regelmatige basis op de hoogte gebracht van privacy issues tijdens hun werkoverleg. In de SHA-nieuwsbrief komt privacy regelmatig aan bod. De gedragsregels ten aanzien van privacygevoelige informatie staan beschreven in het personeelsbeleid van de SHA, in de geest van Artikel 40-AVG. Tijdens het inwerkprogramma dit individueel besproken. In het reglement huisartsen en de informatiefolder voor waarnemers staan de gedragsregels voor de huisartsen beschreven.

In de contracten is een geheim-houdingsverklaring opgenomen. Alleen indien er een behandelrelatie bestaat mag er informatie aangaande een patiënt worden ingezien/opgezocht in Call Manager. Een uitzondering hierop vormen de medewerkers die in het kader van de uitvoering van hun

werkzaamheden toegang moeten kunnen hebben tot patiëntgegevens. Deze medewerkers hebben hiervoor een ‘privacyverklaring’ getekend waarin zij aangeven de toegang alleen voor de aan hun toegewezen werkzaamheden te zullen gebruiken.

Als een triagist een beveiligings-incident veroorzaakt, vindt er een gesprek plaats met haar leidinggevende. Indien aantoonbaar en moedwillig door een triagist een beveiligingsincident wordt veroorzaakt, worden disciplinaire maatregelen getroffen. Deze kunnen uiteindelijk resulteren in ontbinding van het contract. Een dergelijke procedure wordt ook gevolgd indien het een huisarts betreft, alleen vindt in dat geval het gesprek plaats met de directeur en/of de medisch coördinator van de SHA.

Bij uitdiensttreding wordt een procedure gevolgd die ervoor zorgt dat alle rechten van de betreffende medewerker worden ingetrokken. Na het doorlopen van deze procedure heeft de betreffende medewerker geen toegang meer tot ICT-middelen en fysieke ruimtes van de SHA.

8.1 Privacy in de wachtruimte

De SHA is zicht bewust dat de wachtruimte een open ruimte betreft, waardoor gesprekken met of over patiënten voor derden te volgen kunnen zijn. Daarom vinden achter de balie van de SHA geen privégesprekken en gesprekken over patiënten plaats.

9. Informatiebeveiliging

Informatiebeveiliging op de SHA heeft betrekking op het behoud van vertrouwelijkheid, integriteit en beschikbaarheid van (patiënten) informatie binnen de SHA.

- Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.
- Integriteit: het waarborgen van de correctheid en de volledigheid van informatie en de verwerking hiervan.
- Beschikbaarheid/continuïteit: het waarborgen dat geautoriseerde gebruikers op het juiste moment toegang hebben tot informatie.

9.1 Rapportage datalekken

Er is een regeling voor het melden van informatiebeveiliging/privacy incidenten door medewerkers en patiënten, conform Artikel 33,34-AVG. Er is een register waarin de meldingen bijgehouden worden door de kwaliteitsmedewerker. De mogelijke datalekmeldingen en de genomen acties worden ieder kwartaal gerapporteerd in de kwartaalrapportage van de SHA. De werkwijze omtrent datalekken is beschreven in het protocol “melden van datalekken”.

9.2 Toegangsrechten

Binnen de SHA zijn de systeembeheerder (CallManager), office-manager (intranet en Intershift) of de kwaliteitsmedewerker (TPSC) verantwoordelijk voor het toekennen en intrekken van de toegangsrechten tot de diverse informatiesystemen. De toegangsrechten voor de website en intranet zijn opgenomen in het protocol informatievoorziening en communicatie. Overige toegangsrechten voor CallManager, de Telefonie, NTS, The Patient Safety Company (TPSC) en Intershift (roosterprogramma) staan beschreven in bijlage 1. De toegangsrechten voor andere IT-onderdelen worden door de hostingleverancier ingeregeld op aanwijzingen van de systeembeheerder. Welke personen wel/geen toegang hebben tot IT-voorzieningen wordt door de directeur van de SHA vastgesteld.

9.2.1 Proactieve controle op toegang

Maandelijks genereert de systeembeheerder een overzicht met ‘verdachte gevallen’ van inzage in patiëntendossiers in CallManager, conform Artikel 32-AVG. Dit overzicht wordt steekproefsgewijs gecontroleerd door de manager primair proces op mogelijke verdachte zaken. Hiervan vindt rapportage plaats in de kwartaalrapportages.

10. Fysieke ruimtebeveiliging

De SHA is gehuisvest in Ziekenhuis Amstelland (ZHA). Toegang tot de diverse ruimtes wordt geregeld via een pasjessysteem dat door ZHA wordt beheerd. Alle kantoormedewerkers, triagisten, chauffeurs, aangesloten huisartsen en hidha’s krijgen een badge op naam met op de functie toegespitste toegangsrechten. De office-manager beheert de badges en controleert de uitgifte op rechtmatigheid.

11. Camerabeleid

Er zijn camera's aanwezig die beelden registreren van het parkeerterrein, de toegangsdeur, de wachtruimtes en de balie. De beelden worden 7x24 uur bewaard, zoals beschreven in het beveiligingsplan van ZHA. Deze beelden zijn zichtbaar op een monitor in het Call Center. De beelden worden digitaal opgenomen en beheerd door ZHA. Met het ZHA zijn hierover afspraken gemaakt, deze afspraken zijn in het verwerkingsregister gedocumenteerd.

12. Rechten van patiënten

De SHA verplicht zich te houden aan alle relevante wet- en regelgeving met betrekking tot de privacyrechten van de patiënten. Deze rechten staan beschreven in het ‘privacyreglement’, op de website van de SHA en in de informatiefolder voor patiënten.

12.1 Wet geneeskundige behandelovereenkomst (WGBO)

Zorgverleners die vanwege hun beroep met medische gegevens werken, zijn gebonden aan een geheimhoudingsplicht. Dat houdt in dat zij in principe geen gegevens van een patiënt aan anderen mogen verstrekken. Bij toestemming van de patiënt, wettelijke voorschriften of conflict van plichten mag deze informatie wel verstrekt worden. De zorgverleners op de SHA mogen alleen gegevens aan derden verstrekken als dat mag op grond van de AVG en als er een grond is om het medisch beroepsgeheim te doorbreken.

12.2 Verzoek uitoefenen rechten van betrokkenen

De SHA handelt volgens de huidige wet en regelgeving, indien er een verzoek komt van een betrokkene om één of meerdere van onderstaande rechten uit te oefenen. Als het verzoek in strijd is met andere wet en regelgeving kan de SHA een verzoek van een betrokkene weigeren. De SHA zal de motivatie voor de weigering van het verzoek verstrekken aan de betrokkene.

12.3 Recht op informatie over de verwerkingen

Dit heeft de SHA voor patiënten vormgegeven door publicatie van het privacyreglement op de website, algemene informatie over privacy op de website, de privacyfolder in de wachtkamer en informatie op het wachtkamerscherm.

12.4 Recht op inzage

Het recht op inzage staat beschreven in het protocol ‘inzien van patiëntgegevens en verstrekking aan patiënt’.

12.5 Recht op indienen van een verzoek tot correctie of aanvullen van gegevens

Het recht op het indien van een verzoek tot correctie of verwijdering van gegevens voor de patiënten is beschreven in het protocol ‘rectificatie van patiëntgegevens’.

12.6 Recht op beperking van de verwerking

Het recht op beperking van de gegevensverwerking door patiënten staat beschreven in het protocol ‘vernietiging van patiëntendossiers’.

12.7 Recht op bezwaar maken tegen bepaalde wijze van gebruik van gegevens

Dit recht staat beschreven in het protocol ‘vernietiging van patiëntendossiers’.

12.8 Recht om vergeten te worden

Deze werkwijze staat beschreven in het protocol ‘Vernietiging patiëntendossier’.

12.9 Recht op het overdragen van persoonsgegevens (dataportabiliteit)

Het recht op overdracht van patiëntgegevens (dataportabiliteit) is vastgelegd in het protocol ‘Inzien van patiëntgegevens en verstrekking aan patiënt’.

12.10 Opname gesprekken door een patiënt/klager

De SHA gaat niet akkoord dat patiënten of andere gespreksdeelnemers een gesprek wat we met elkaar voeren opnemen. Indien de patiënt dit wenst zal er een gespreksverslag worden gemaakt, zodat de patiënt op een later tijdstip nog kan nalezen wat er in het gesprek besproken is.

13. Risicobeoordeling

De SHA heeft het volgende uitgangspunt: een continu proces inrichten van het identificeren van processen en systemen die van vitaal belang zijn in de zorg, analyseren en behandelen van risico’s. De basis van goede informatiebeveiliging is dat de SHA regelmatig een risicobeoordeling uitvoert en de geconstateerde risico’s behandelt. De risicobeoordeling zal iedere 3 jaar plaatsvinden, tenzij er een aanleiding is om eerder een risicobeoordeling uit te voeren (bij nieuwe of sterk veranderde informatiesystemen). De verantwoordelijkheid voor het organiseren van en de inhoud van de beoordeling ligt bij de directie. De betrokken medewerkers bij de risicobeoordeling zijn een afspiegeling van de SHA. Indien nodig worden ook leveranciers van informatiesystemen betrokken bij de beoordeling. Op basis van de rapportage wordt besloten of het risico geaccepteerd wordt, behandeld wordt door middel van maatregelen, vermijdt of verlegt. Deze risico’s worden opgenomen in een werkplan waarin de genomen acties en verantwoordelijke personen bijgehouden worden. Na afloop van de risicobeoordeling wordt vastgelegd wat er goed en minder goed ging tijdens de beoordeling. Deze informatie wordt gebruikt als input voor de volgende risicobeoordeling.

13.1 Data Protection Impact Analyse (DPIA)

Een ‘Data Protection Impact Assessment’ (DPIA) wordt uitgevoerd op de SHA, om de actuele situatie van de gegevensbescherming in kaart te brengen. De SHA werkt hierbij volgens de stappen die opgenomen zijn in de handreiking van InEen. Dit levert als resultaat op dat de SHA weet wat zijn beveiligings- en privacy risico’s zijn. Tevens zorg dit voor grotere zekerheid dat de SHA hiertegen passende maatregelen heeft genomen.

Bijlage 1. Autorisatieschema's

Onderstaand overzicht is het uitgangspunt voor de toegang tot de persoonsregistratie. Per categorie wordt aangegeven vanuit welke functie welk type van activiteiten mag worden ondernomen. De SHA houdt een lijst bij van namen van functionarissen die werkzaam zijn, deze lijst is op verzoek in te zien.

Medewerker	Pc's / Laptops	Call Manager	NTS	Telecom (telefonie)
Administratief (AO) medewerker	Inloggen op eigen account op pc-callcenter geen installatie rechten op pc's.	Beperkte rechten.	Gebruiker rechten	nvt
Chauffeur	Nvt	Beperkte rechten	Nvt	Nvt
Deelnemend huisarts, waarnemend huisarts, HIDHA, AIOS, medisch coördinator	Inloggen, geen installatie rechten op pc's.	Beperkte rechten & toegang tot beschikbare RSP.	Nvt	Geen account
Directeur	Inloggen, geen installatie rechten op pc's. Heeft een eigen laptop.	Nvt	Nvt	Nvt
ICT- adviseur	Inloggen, geen installatie rechten op pc's. Wel op eigen laptop	Alle rechten, inclusief het zelf toekennen van rechten	Nvt	Eigen account en alle rechten in adm. Tool Telecom.
Interne auditor	Nvt	Beperkte rechten.	Nvt	Nvt
Kwaliteitsmedewerker	Inloggen, geen installatie rechten op pc's. Wel op eigen laptop	Beperkte rechten	nvt	Geen account
Leidinggevend triagist	Inloggen, geen installatie rechten op pc's. Wel op eigen laptop	Beperkte rechten.	Rapportage	Eigen account (niet onder eigen naam, maar onder nummer)
Manager primair proces	Inloggen, geen installatie rechten op pc's. Wel op eigen laptop	Beperkte rechten.	Gebruiker rechten	Eigen account & toegang tot uitluistermodule
Office-manager	Inloggen, geen installatie rechten op pc's	Alle rechten, inclusief het zelf toekennen van rechten	Nvt	Eigen account
Systeembeheerder	Inloggen, geen installatie rechten op pc's. Wel op eigen laptop	Alle rechten, inclusief het zelf toekennen van rechten	Alle rechten	Eigen account en alle rechten in adm. Tool Telecom.
Triagist	Inloggen, geen installatie rechten op pc's.	Beperkte rechten.	Gebruiker rechten	Eigen account (niet onder eigen naam, maar onder nummer)
Uitzendkracht, ZZP'er, junior triagist, stagiaire BOL/BBL	Inloggen, geen installatie rechten op pc's.	Beperkte rechten.	Gebruiker rechten	Eigen account (niet onder eigen naam, maar onder nummer)

De administratief ondersteuner heeft met gereduceerde rechten toegang tot CallManager door middel van inloggen met naam en wachtwoord. Tevens is er een eigen inlog voor de vaste chauffeurs.

Functionaris	**Stamgegevens**	**Medische gegevens**	**Financiële gegevens**
AO -medewerker*	M	G	G
Interne auditor	R	R	G
Chauffeur	R	G	G
Directeur	G	G	V
Financieel medewerker	R	R	V
Huisarts* Evenals medisch coördinator	M	M	G
Huisarts in opleiding*	M	M	G
ICT-adviseur	R	R	G
Kwaliteitsmedewerker	R	R	G
Leidinggevend triagist*	M	M	G
Manager primair proces	M	M	G
Office-manager	M	R	G
Systeembeheerder	R	G	G
Triagist*	M	M	G

Toelichting	
Stamgegevens	Personalia c.q. identificatiegegevens
Medische gegevens	Medische, sociale en psychologische gegevens
Financiële gegevens	Financiële c.q. administratieve gegevens
G	Geen toegang
R	Raadplegen
M	Raadplegen, invoeren, muteren, corrigeren en aanvullen
V	Raadplegen, invoeren, muteren, corrigeren, aanvullen en vernietigen
*	De toegang geldt alleen indien er sprake is van een behandelrelatie met de patiënt. Standaard hebben alle huisartsen toegang tot de overzichten van patiënten bij wie hij/zij direct bij de zorgverlening betrokken is geweest. Dit kan tot 24 uur na de behandeling.

Onderstaande tabel geeft het overzicht van de bevoegdheden in Intershift (roosterprogramma). Door de administrators is in te zien wie onder welke groep gebruikers valt.

Bevoegdheden in Intershift (roosterprogramma)		
	Rooster voor huisartsen	**Rooster voor triagisten**
Administrator	Zelfde als planner hagro, maar met de extra functionaliteit: Plannen hagrorooster Bijhouden extra uren Managementoverzichten Gegevens exporteren naar Excel Overzicht patiënten aantallen Analyse roosters Correctiebedragen opvoeren Declaraties aanmaken Betalingen uitvoeren Onderhoud van huisartsen Onderhoud van waarnemers/hidha's Onderhoud van gebruikers Onderhoud van dienstcodes Onderhoud van selecties Onderhoud van Huisartenpost/Hagro's Onderhoud van Tarieven Onderhoud van Feestdagen Instellingen wijzigen	Onderhoud van alle codetabellen Onderhoud van de CAO en ORT gegevens (optioneel) Onderhoud van contractgegevens Afsluiten van maandplanningen Importeren van date (optioneel) Management informatie (optioneel) Exporteren data Exporteren data ten behoeve van betalingen (optioneel) Onderhoud van extra vakantie (optioneel) Onderhoud van gebruikers -en medewerkersgegevens
Financieel medewerker	Zelfde als huisarts, maar met de extra functionaliteit: Managementoverzichten Exporteren naar Excel Correctiebedragen opvoeren Declaraties aanmaken en beheren Betalingen uitvoeren	
Gastgebruiker huisartsenrooster	Huisartsenrooster (evt. beperkt tot 1 hagro) Inzetten waarnemers op diensten N.C/V en A.C3	Nvt
Huisartsen	Homescherm Inkijken eigen rooster Inkijken huisartsrooster Inkijken hagrorooster Ruilingen beheren Prikbord Eigen gegevens Adressen huisartsen Adressen waarnemers Overzicht dienstcodes Declaratieoverzicht	Nvt
Planner HAP Huisartsenrooster	Zelfde als huisarts, maar met de extra functionaliteit: Plannen huisartsrooster	Nvt
Planner Triagistenrooster	Nvt	Plannen van het rooster (handmatig en automatisch) Inzien van contract gegevens (uren en contractduur) van medewerkers

		Inzien van vakantieuren kaarten van medewerkers Afsluiten van maandplanningen Onderhoud van dienstcodes en benodigde diensten
Triagisten	Nvt	Homescherm Inkijken eigen rooster Overzicht rooster huisartsen van dezelfde dag incl. telefoonnummers huisartsen Inkijken assistentenrooster Eigen ruilingen beheren Eigen diensten accorderen Prikbord Eigen gegevens Adressen assistentes Verjaardagen assistentes Overzicht dienstcodes Onregelmatigheidstoeslag
Waarnemend huisartsen	Homescherm Inkijken eigen rooster Inkijken huisartsrooster Eigen gegevens Overzicht dienstcodes	

Toegangsrechten The Patient Safety Company (TPSC).

Medewerker	**VIM-melding via formulier intranet**	**Dienstoverdracht**	**VIM en ARBO**	**Klachten**
Chauffeur	X	Geen toegang	Geen toegang	Geen toegang
Deelnemend huisarts, waarnemend huisarts, HIDHA, AIOS	X	Geen toegang	Geen toegang	Geen toegang
Directeur	X	Lezen	Lezen	Lezen
ICT- adviseur (beheerder)	X	Lezen en schrijven	Geen toegang	Geen toegang
Klachtenfunctionaris en vervanger	Geen toegang	Geen toegang	Geen toegang	Lezen en bewerken
Kwaliteitsmedewerker (beheerder)	X	Lezen en schrijven	Lezen en bewerken	Lezen en bewerken
Manager primair proces	X	Lezen en schrijven	Lezen en bewerken	Lezen en bewerken
Medisch coördinator	X	Geen toegang	Lezen en bewerken	Lezen en bewerken
Office-manager	X	Lezen	Geen toegang	Lezen en bewerken
Systeembeheerder (beheerder)	X	Lezen en schrijven	Geen toegang	Geen toegang
(leidinggevend) Triagist, uitzendkracht, ZZP'er, junior triagist, stagiaire BOL/BBL	X	Schrijven	Geen toegang	Geen toegang