Huisreglement informatieveiligheid en gegevensbescherming

1. Het belang van informatieveiligheid en gegevensbescherming

Het woonzorgcentrum wil voor al haar bewoners, familie, betrokken actoren (bv vrijwilligers) en medewerkers een comfortabele omgeving bieden in combinatie met professionele zorg en werkomgeving.
Een aangenaam leefklimaat en deskundige zorg staan hierbij centraal. We hebben hierbij oog voor respect, menselijke warmte, persoonlijke aandacht en privacy.
Ons zorgcentrum staat garant om de gegevens die we van onze bewoners, enz. verzamelen, te verwerken met de grootste aandacht voor privacy. We streven continu naar verbetering, met als doel een veilige informatieomgeving te creëren.

In het bijzonder willen we de gegevens van onze bewoners, enz. beschermen tegen:

- verlies: gegevens zijn niet meer beschikbaar
- lekken: gegevens komen in verkeerde handen terecht
- fouten: gegevens zijn niet correct, bijvoorbeeld verouderd of onvolledig
- niet toegankelijk: op het moment van de zorg zijn gegevens niet toegankelijk
- onterecht inkijken: ingekeken door personen die hiertoe niet gemachtigd zijn
- het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde
- verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen

De directie wil beroep doen op iedereen die betrokken is bij het elektronisch verwerken van persoonsgegevens om samen, vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle zorg aan te bieden, de verwerking van de gezondheidsgegevens van onze bewoners, enz. correct te laten verlopen.

Dit beleidshandboek (onderdeel van het kwaliteitshandboek)

- dient als norm voor het verwerken van de persoonsgegevens van onze bewoners, enz.
- is een leidraad voor alle verwerkingsprocessen,
- biedt een referentienorm voor audit en controle,
- biedt elke bewoner, medewerker en externe een inzage in het veiligheidsbeleid en de manier waarop we omgaan met gevoelige persoonsgegevens.

Deze tekst is geschreven voor iedereen die een beleidsfunctie heeft binnen het woonzorgcentrum. Ze gebruiken (delen van) dit beleidshandboek voor het ontwerpen van procedures en richtlijnen voor medewerkers en externen, zoals ICT-leveranciers.

De relevante onderdelen van dit beleidshandboek worden verwerkt in overeenkomsten met personeel en leveranciers

2. DE ORGANISATIE VAN INFORMATIEVEILIGHEID EN GEGEVENSBESCHERMING

Bevoegdheid

Als verantwoordelijke voor de verwerking, ligt de bevoegdheid van dit veiligheidsbeleid bij het woonzorgcentrum, vertegenwoordigd door de algemeen directeur, mevrouw Hilde Hemelsoen.

Zij is verantwoordelijk voor het formuleren van de beleidsprincipes en voor de naleving ervan binnen het woonzorgcentrum.

Verantwoordelijke uitvoerder

De algemeen directeur, dagelijks verantwoordelijke, is bevoegd om beslissingen te nemen die betrekking hebben op volgende aspecten:

- De risicoanalyse en bijhorende methodiek;
- Het ontwikkelen van het informatieveiligheidsbeleid en de bijhorende richtlijnen;
- De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan)
- De structurele reactie op informatieveiligheidsproblemen en –adviezen (binnen de 3 maanden);

Plaats

Het beleidshandboek wordt geïntegreerd in het kwaliteitsmanagement van het woonzorgcentrum, onder het toeziend oog van de stafmedewerker kwaliteitszorg.

De veiligheidsconsulent/data protection officer (DPO)

De inhoudelijke opvolging van het veiligheidsbeleid en de bescherming van de persoonsgegevens (DPO) ligt bij de veiligheidsconsulent/DPO. Hij/zij voert deze taak uit volgens de bepalingen in het Vlaams decreet van 15 mei 2009 betreffende veiligheidsconsulenten, o.a. de richtlijnen van Belrai inzake veiligheidsconsulenten, art. 39 van de gegevensbescherming e.a. reglementering die van toepassing is.
Het woonzorgcentrum legt de identiteit (en eventuele wijzigingen) van de veiligheidsconsulent/DPO voor aan de Vlaamse Toezichtcommissie ter beoordeling.
De veiligheidsconsulent/DPO rapporteert aan de directeur van het woonzorgcentrum en is meer in het bijzonder belast met:

- Adviezen en aanbevelingen voorleggen aan de directeur;
- Opdrachten uit te voeren op vraag van de directeur;
- Bevorderen van de bewustwording van alle actoren binnen het woonzorgcentrum;
- Ziet toe op de naleving van het veiligheidsbeleid binnen het woonzorgcentrum;
- Documenteert het veiligheidsbeleid, in overleg met de kwaliteitsmedewerker (verantwoordelijke medewerker) en volgens dezelfde methodiek;

- Stelt het veiligheidsplan op voor een periode van 3 jaar en waakt over de uitvoering ervan;
- Stelt een jaarverslag op met de vorderingen van het veiligheidsplan en legt dit voor aan de directie (of team leidinggevenden);
- Registreert overtredingen en maakt deze, samen met een advies, over aan de directeur.

De medewerker

Iedereen (intern of extern) die gegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, …), doet dit volgens de beleidsprincipes uit dit beleidshandboek.

De gebruiker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Is verantwoordelijk voor de gegevens van bewoners die hij/zij verwerkt;
- Voert de veiligheidsrichtlijnen uit tijdens zijn/haar verwerkingsopdracht;
- Verwerkt enkel die gegevens die horen bij de taak;
- Draagt zorg voor de gegevens;
- Meldt inbreuken;
- Leeft artikel 458 van het Strafwetboek na: de gebruiker respecteert het beroepsgeheim.

Diensthoofd

Bijkomend aan de verantwoordelijkheden van de medewerker, ziet het diensthoofd toe op de goede uitvoering van de veiligheidsbepalingen. Het volgt de veiligheidsrichtlijnen op en informeert de medewerkers hierover. Het diensthoofd zorgt voor een veiligheidscultuur in zijn/haar team en onderhoudt deze, bijvoorbeeld door het bespreken van de beleidsrichtlijnen op het teamoverleg. Het diensthoofd ondersteunt controleactiviteiten, bijvoorbeeld door het controleren van logging in het elektronisch bewonersdossier.

Coördinerend en raadgevend arts

Op vraag van de veiligheidsconsulent/DPO en de algemeen directeur bepaalt de coördinerend arts veiligheidsprincipes voor de bescherming van de medische persoonsgegevens van de bewoners. Het principe van individuele verantwoordelijkheid binnen ieders zijn bevoegdheidsdomein wordt hierin gevolgd.

Behandelend arts

Naast de veiligheidsprincipes, zoals bepaald voor de medewerker, is de behandelend arts verantwoordelijk voor het afleveren van een correct medisch dossier.

ICT-medewerker en key-gebruiker

De ICT-medewerker en de verantwoordelijke voor de gebruikers (key-gebruiker) zijn, in toevoeging van de verantwoordelijkheden voor de gebruiker, verantwoordelijk voor:

- De implementatie van de technische maatregelen;
- Veiligheidsinstellingen te implementeren in lijn met dit beleidshandboek;

- Veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen te melden aan de veiligheidsconsulent/DPO;
- Fungeert als expert. Vanuit deze rol neemt hij/zij deel aan de identificatie zowel als aan de remediëring van de informatieveiligheidsrisico's;
- De gedragscode naleven.

ICT-leverancier

De ICT-leverancier heeft dezelfde verantwoordelijkheden als deze van een ICT-medewerker.

Bijkomstig:

- Wijst hij op veiligheidsrisico's van geleverde toepassingen;
- Wijst de leverancier op de op te nemen veiligheidstaken;
- Streeft de leverancier een transparant veiligheidsbeleid na door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

3. De scope van de informatieveiligheid en de gegevensbescherming

Dit beleidshandboek verdiept zich in de informatieveiligheid bij zowel het lokaal verwerken als het delen van gegevens met verschillende actoren in de gezondheidssector.
We hebben in dit beleid aandacht voor de omgang met persoonsgegevens van onze bewoners, familie, medewerkers en andere betrokken actoren.
Daarnaast, in het kader van decreet gegevensdeling en de digitalisering van de woonzorgcentra (het eWZC project), bevat dit beleidshandboek ook bepalingen voor de uitwisseling van gezondheidsgegevens met actoren in de gezondheidszorg. Op die manier confirmeren we bijvoorbeeld ook de bepalingen rond informatieveiligheid, zoals deze zijn opgenomen in de aansluitingsvoorwaarden voor het Vitalink platform.
Het veiligheidsbeleid is van toepassing op alle medewerkers van het woonzorgcentrum, zowel medewerkers in dienstverband als medewerkers die via andere overeenkomsten deelnemen aan de gegevensverwerking (zelfstandige zorgverleners, stagiairs en vrijwilligers).
De bepalingen van dit veiligheidsbeleid worden opgenomen in de contracten en kenbaar gemaakt via bewustwordingssessies.
Gezien de belangrijke rol van de ICT-leveranciers bij het opzetten van de ICT-omgeving om gegevens te verwerken, legt het beleidshandboek hiervoor ook de beleidsprincipes vast.
Het woonzorgcentrum tracht de beleidsprincipes in dit handboek ook te gebruiken als richtlijn in de zorgnetwerken waaraan de organisatie deelneemt. Op die manier streven we naar een coherent veiligheidsbeleid, samen met onze partners.