INFORMATIEVEILIGHEID & PRIVACY 2.0

En hoe Amstelring hiermee omgaat

Versie 2.0

Auteurs: Leden stuurgroep Informatieveiligheid
Vastgesteld door: Raad van Bestuur Amstelring
Advies: LMO, Stuurgroep Informatieveiligheid, CCR, OR
Datum aangemaakt/herzien:
Status: definitief

Inleiding

De visie van Amstelring is: samen zorg dragen voor kwaliteit van leven, op basis van gelijkwaardigheid en met respect voor ieders rol. De kaders waarbinnen wij werken zijn: betekenisvolle zorg, leuk werk en een financieel gezonde organisatie. Hiervan afgeleid is de koers voor de inzet van digitale middelen:

- Iedere medewerker van Amstelring is digitaal vaardig en wordt ondersteund door technische middelen die op elkaar zijn afgestemd. Deze zijn 24/7 beschikbaar, snel en begrijpelijk.
- De medewerker wordt dicht bij de cliënt ondersteund met digitale middelen.
- Het gebruik van digitale middelen heeft geen handleidingen nodig.
- Printen, faxen en scannen is niet nodig.
- De informatie in de systemen is betrouwbaar en beschikbaar voor wie en wanneer dat nodig is.

Ons **privacy statement**: Privacy vinden wij heel belangrijk. Zorgvuldig omgaan met persoonsgegevens is bij Amstelring onderdeel van goede zorg en goed werkgeverschap. Medewerkers van Amstelring zijn zich bewust van en handelen naar de actuele wetgeving rondom privacy. Jij gaat vertrouwelijk om met persoonsgegevens en krijgt (en neemt) alleen toegang tot data die nodig is voor je werk.

Informatiebeveiliging gaat om de zaken die Amstelring geregeld heeft zodat de medewerkers doorlopend betrouwbare informatie krijgen voor hun werkzaamheden en dat deze informatie wordt beschermd tegen onbedoeld verlies of misbruik. Privacy gaat specifiek over het beschermen van persoonsgegevens (van medewerkers en cliënten) zodat geen misbruik kan worden gemaakt van deze gegevens.
Dit organiseren we door middel van technische maatregelen, autorisaties en toegang en afspraken met onze leveranciers, controles door applicatiebeheer en controles die de medewerkers zelf doen in de werkprocessen (gebruikerscontroles). Amstelring volgt de NEN-normeringen en specifiek de NEN7510.

Het begint altijd met ons eigen gedrag. Hier kan je lezen wat de afspraken zijn waar we ons aan houden en wat te doen wanneer het toch een keer mis gaat.

We zien dat de risico’s toenemen met de tijd en dat we daardoor ook strenger moeten worden in het beleid.

Digitaliseringsbeleid en Digitale governance

Voor het beleid op Informatieveiligheid beschreven wordt, wordt hier eerst ingegaan op beleid en strategie van Amstelring op digitalisering en daaraan verwant, de digitale governance. Kortweg wordt met dit laatste bedoelt: wie neemt de besluiten over de digitalisering en wie is waarvoor verantwoordelijk?

Van IT-beleid naar beleid op digitalisering

Voor Amstelring betekent de digitale transformatie dat de nadruk ligt op het eenvoudig maken van de IT-omgeving voor de professional met een gestandaardiseerde applicatie-omgeving en werkplek, waarmee ruimte wordt gecreëerd voor experimenteren en innoveren. Afgeleide doelen zijn het voorkomen van een gefragmenteerd IT-landschap en dubbelingen in functionaliteit.
De IT-strategie stamt uit 2015 en is later aangevuld met uitwerkingen op de verschillende onderwerpen, zoals 'Datagedreven werken', 'Een fijne en rustige omgeving door technologie' en 'Vervolg Infrastructuur'. Deze wordt verder aangevuld op de verschillende deelonderwerpen van de digitale innovatie en transformatie van Amstelring.
Een voorstel voor digitalisering wordt vergezeld van een analyse op de volgende aspecten:

1. Functionaliteit met eventueel een vergelijking tussen verschillende oplossingen.
2. IT of digitale strategie, samengevat betekent dit dat we geen dubbele functionaliteit aanschaffen, een simpel it-landschap behouden -product past hierbinnen, dus werkt met Chrome-, Cloud-only, Saas-only en dus standaard oplossingen in plaats van maatwerk, betrouwbare leverancier van voldoende omvang, innovatief en ondersteunend aan het werk van de professional.
3. Informatieveiligheid: hiervoor hebben we het proces van de Risk Impact Assessment, daarover verder meer informatie.
4. Financieel: het voorstel gaat gepaard met een business case. De werking daarvan is beschreven in dit document (link toevoegen naar document van Mike Pompe).

Er is altijd spanning tussen het gebruik van standaarden en maatwerk. Het zoeken van een balans tussen de wensen van de organisatie en efficiënte IT doen we samen. Ditzelfde geldt voor de zoektocht naar een betrouwbare infrastructuur, die daarnaast ook flexibel meebeweegt met de organisatie en innovatief wil zijn.

Centrale regie in samenspraak met de organisatie

De digitale governance is zo ingericht dat de organisatie optimaal en dus de professional optimaal wordt ondersteund, maar op zo'n manier dat fragmentatie wordt tegengegaan en informatieveiligheid gegarandeerd kan worden.
Regie is nodig omdat we anders de eisen die extern aan ons worden gesteld (denk aan de autoriteit persoonsgegevens (AP) en de inspectie gezondheidszorg en jeugd (IGJ) maar ook dichterbij; onze cliënten, als het gaat om beschikbaarheid en beveiliging van de gegevens in het dossier) niet of alleen tegen onevenredige kosten, kunnen waarmaken.
Van belang is dat de inzet van digitale technologie niet altijd volgend is op de wensen van organisatieonderdelen, omdat dan het risico bestaat van suboptimalisatie. De afwegingen worden gemaakt in overleg met de organisatie. Hiertoe worden voorstellen voor digitalisering voorgelegd volgens de processen 'incident en change management' en 'ontwikkeling en beheer informatievoorziening'.
De volgende (stuur-)groepen zijn ingericht om de veranderingen te volgen en te besluiten:

1. Primaire applicaties: Integraal Overleg Zorgapplicaties
2. Secundaire applicaties: Stuurgroep Afas, tenzij en Stuurgroep BI
3. Hardware en software op gebied van security, maar ook bijv. netwerksoftware: Stuurgroep Informatieveiligheid & Privacy
4. Voor overige technologie: Zorgtechnologie en Telefonie.

De voorstellen voor de inzet van digitale technologie worden altijd gedaan in samenspraak en met een vertegenwoordiging van gebruikers. In de (stuur-)groep zit altijd een vertegenwoordiging van RVE-management, regiehouder IT, innovatie en data en adviseurs van de verschillende terreinen. Daarna worden wijzigingsvoorstellen ter besluitvorming voorgelegd aan de raad van bestuur.

Regionale context

De grenzen van ons applicatielandschap vervagen; het gaat niet alleen meer om applicaties van Amstelring, maar het steeds meer gebruiken van applicaties die binnen de regionale netwerken waarin Amstelring deelneemt in gebruik zijn of worden genomen. De visie van Amstelring hierop is dat meegewerkt wordt met de initiatieven die bijdragen aan eigen regie van onze cliënten en het werk voor onze zorgprofessionals makkelijk maken.
Besluitvorming over deelname vindt plaats met de professional, regiehouder it en het bestuur. De voorstellen worden ook gedeeld en besproken in de hierboven genoemde (stuur-)groepen.

Hoe digitaal transformeren

Digitale transformatie wordt vormgegeven op een manier die bij ons past: iteratief, verschillende aanpak per verandering (soms agile, soms watervalmethode), in cocreatie met de organisatie en soms in een proces van kleine stapjes.
Vaak is de digitale transformatie een onderdeel van een ander programma. Hierin wordt aangesloten bij de gekozen aanpak van het programma. Adviseurs op het terrein van digitalisering sluiten aan bij deze programma's.

Verantwoordelijkheden informatieveiligheid & privacy

NEN 7510 II-06.1.1 Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.

We zijn allemaal verantwoordelijk voor informatieveiligheid & privacy. We willen continu verbeteren, ook op dit vlak. Dit betekent dat elk incident ook een leermoment is. Aangebrachte verbeteringen zijn input voor een goede en doorlopende verbetercyclus: plan, do, check, act.

Iedereen bij Amstelring is verantwoordelijk voor het veilig omgaan met informatie en het bewaken van de persoonsgegevens waar hij/zij mee te maken heeft en is dus ook zelf verantwoordelijk om te handelen naar de afspraken die in dit document staan. In dit document gebruiken we de term 'medewerker'; hieronder wordt ook verstaan de vrijwilliger, lid cliëntenraad, lid Raad van Toezicht, uitzendkracht/externe of stagiaire.

Hieronder staan meer gespecialiseerde functies:
Applicatie- en systeembeheerders
De applicatie- en systeembeheerders zijn verantwoordelijk om de autorisatie en toegang tot de applicaties waar hij /zij verantwoordelijk voor is, zo in te richten dat voldaan wordt aan de afspraken in dit document.

Functionaris Gegevensbescherming (FG)
Verantwoordelijk voor het toezicht op de inrichting van de processen rondom privacy. Daarnaast heeft de FG een adviserende en toezichthoudende functie voor privacy-gerelateerde onderwerpen. Ook heeft Amstelring een *Privacy Officer*. De Privacy Officer adviseert gevraagd en ongevraagd over onderwerpen rondom de privacy en coördineert de melding van datalekken.

Security Consultant
Deze functie dient nog nader gedefinieerd te worden.

Proceseigenaar
Deze heeft de verantwoordelijkheid voor onder meer de autorisatiematrix.

RVE manager
De RVE manager is integraal verantwoordelijk voor de kwaliteit en financiën binnen de eigen RVE. Daar hoort ook de (decentrale) informatieveiligheid bij. De RVE manager draagt zorgt dat de medewerkers van de RVE uitvoering geven aan het

informatieveiligheidsbeleid. De RVE-manager controleert de autorisaties van de medewerkers in ieder geval 1 keer per jaar en ieder kwartaal de gesignaleerde uitzonderingen.

Regiehouder IT, innovatie en data
Binnen de organisatie zijn de verantwoordelijkheden voor de technische maatregelen belegd bij de regiehouder IT, innovatie en data. Deze regiehouder is verantwoordelijk om ook toe te zien of de werking van de technische, organisatorische en specifieke maatregelen die genomen zijn om het beleid van digitalisering, de digitale governance en het informatieveiligheidbeleid uitgevoerd worden. Bij calamiteiten zal de regiehouder een trekkende rol hebben in opvolging.

Stuurgroep Informatieveiligheid
Opstellen, evalueren en bijstellen van de afspraken rondom informatieveiligheid en verantwoordelijk voor risico-afwegingen op dit vlak. De leden van de stuurgroep zijn adviseurs op het gebied van Audit, Security, HR, FG, Security Consultant, regiehouder IT en lid RvB.

Raad van Bestuur
De raad van bestuur is conform de Governancecode zorg verantwoordelijk voor het beheersen van de risico's verbonden aan de strategie en de verschillende activiteiten van de zorgorganisatie. De raad van bestuur draagt zorg voor goede en hanteerbare interne risicobeheersings- en controlesystemen, de bemensing daarvan en de werking van die systemen. De Raad van Bestuur is verantwoordelijk voor het vaststellen van het beleid en neemt deel aan de stuurgroep informatieveiligheid.

Raad van Toezicht
De raad van toezicht is verantwoordelijk voor het toezicht op het handelen en beleid van de raad van bestuur en moet deze met raad en daad bijstaan en moet worden geïnformeerd en zich laten informeren over zaken die hiervoor van belang zijn, waaronder het informatieveiligheidsbeleid. Daarnaast is statutair de voorafgaande goedkeuring van de raad van toezicht vereist voor (meerjaren)beleidsplannen.

Optioneel Ambassadeur AVG
Binnen een RVE kan een ambassadeur AVG medewerkers helpen bij vraagstukken m.b.t. informatieveiligheid en vooral privacy/de AVG. De ambassadeur heeft een adviserende rol, een rol als vraagbaak, maar niet een besluitvormende rol. Binnen de RVE ligt de verantwoordelijkheid voor de uitvoering van het informatieveiligheidsbeleid binnen de vastgestelde kaders bij de RVE manager.

Privacybeleid Amstelring

Privacyverklaring

De (externe) privacyverklaring die gepubliceerd is op www.amstelring.nl is onderdeel van het Privacybeleid.

Het Amstelring Privacybeleid is bestemd voor alle personen werkzaam binnen de Stichting Amstelring (en de andere rechtspersonen die hieronder vallen) en is van toepassing op alle persoonsgegevens die binnen Amstelring worden verwerkt. Het beleid beschrijft de maatregelen op het gebied van privacybescherming.

Het Privacybeleid ondersteunt het principe van 'Privacy-by-design': al in de beginfase(s) van een project en bij het ontwikkelen van producten of diensten wordt rekening gehouden met de bescherming van persoonsgegevens.

De uitgangspunten in dit beleid zijn gebaseerd op wettelijke vereisten: de Algemene Verordening Gegevensbescherming (AVG), een Europese verordening voor bescherming van persoonsgegevens en andere specifieke nationale wet- en regelgeving.
De basis van het privacybeleid van Amstelring kenmerkt zich door het vastleggen van: zo min mogelijk gegevens, het doel van de vastlegging en de bekendheid bij betrokkenen hiervan.

Hier wordt dit nog verder uitgelegd:

Dataminimalisatie
De wet zegt dat persoonsgegevens - gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt - 'toereikend, terzake dienend en niet bovenmatig moeten zijn'. Dit betekent dat Amstelring bij het uitoefenen van haar werkzaamheden zo weinig mogelijk persoonsgegevens moet gebruiken. Daardoor is bij een eventueel datalek het risico voor betrokkenen kleiner, omdat er minder gegevens zijn die verloren kunnen gaan.

Doelbinding
Voor iedere verwerking van persoonsgegevens moet vooraf duidelijk worden vastgesteld waarvoor de persoonsgegevens worden gebruikt. Dit bepaalt welke persoonsgegevens Amstelring mag verwerken, hoe lang Amstelring gegevens mag gebruiken en waarvoor Amstelring de gegevens in de toekomst mag gebruiken.

Informeren
Betrokkenen moeten altijd goed en duidelijk worden geïnformeerd over de verwerking. Zij moeten weten wat voor persoonsgegevens worden verwerkt, door

wie en wat er met de gegevens gebeurt. Zo houdt de betrokkene controle over de eigen persoonsgegevens.

De privacy-afspraken

Het vastgestelde privacybeleid van Amstelring staat op de website van Amstelring. Amstelring verwacht dat iedereen werkzaam bij Amstelring op de hoogte is van de belangrijkste regels en (hoofdpunten uit de) wetgeving rondom privacy.

Je aan de spelregels houden betekent dat je je aan de volgende privacy-afspraken houdt:

1. Je deelt alleen persoonsgegevens met andere partijen wanneer dit nodig is voor de uitvoering van jouw dienstverlening of wanneer dit verplicht is vanwege (andere) wetgeving. Je zult nooit persoonsgegevens verkopen aan derden.

   Alle medewerkers van Amstelring zijn wat betreft cliëntgegevens ook gebonden aan het (medisch) beroepsgeheim.

2. Je deelt alleen persoonsgegevens met collega's wanneer dit nodig is voor de dienstverlening aan jouw cliënten. Alleen wanneer het nodig is voor de behandeling zullen medische gegevens gedeeld worden tussen medewerkers betrokken bij deze behandeling, en dan altijd zo min mogelijk gegevens en altijd per beveiligde e-mail naar individuen en niet naar groepsmailboxen of distributielijsten. Dit betekent dat je alleen in dossiers kijkt waar je vanuit je functie bij moet. Mocht je meer toegang hebben, dan wordt er van je verwacht dat je alleen in de dossiers kijkt waar je vanuit je functie bij moet. Tevens wordt van je verwacht dat wanneer je teveel ziet, je dit meldt bij applicatiebeheer en informatieveiligheid@amstelring.nl.

   Er mag niet gekeken worden in een dossier van bijvoorbeeld de moeder van je buurvrouw die zorg of behandeling ontvangt van Amstelring waar jij niet bij betrokken bent.

3. Amstelring stelt vooraf de doeleinden en grondslag voor de verwerking van persoonsgegevens vast, in lijn met de AVG. Je gebruikt persoonsgegevens niet voor andere doeleinden of grondslagen.

   Medewerkers mogen een mailadres dat verzameld is om uitnodigingen voor een informatieavond te versturen niet gebruiken om bijvoorbeeld reclame te versturen.

4. Je voldoet aan de juiste voorwaarden bij het gebruik van de grondslag ‘toestemming’.

   Alle cliënten vullen een duidelijke toestemmingsverklaring in voordat foto’s van hen worden gepubliceerd. Ze kunnen hun toestemming altijd intrekken.

5. Bij verwerking van alle persoonsgegevens volg je de instructies om te voldoen aan organisatorische en technische eisen. Alle systemen hebben goede toegangsautorisaties, Amstelring controleert deze regelmatig.

   Je gebruikt je telefoon (privé of van Amstelring) om op een tweede manier (naast inlognaam en wachtwoord) de applicatie te laten weten dat jij het bent.

6. Als jij of je team besluit om nieuwe IT systemen of processen te implementeren, bestaande systemen of processen aan te passen (of te beëindigen), moeten de **privacy, beveiliging en IT risico’s** eerst in kaart worden gebracht en eventueel risicoverlagende maatregelen getroffen moeten worden alvorens de wijzigingen gemaakt mogen worden. Wil je meer weten over wat je dan moet doen, klik dan hier.
   Je wilt Sillo gebruiken om cliëntgegevens te delen met de specialist van het ziekenhuis en je wilt de app downloaden. Alvorens dit te doen start je een onderzoek naar de risico’s (RIA) of neem je contact met het ISA.

7. Bij beleidsonderwerpen die van invloed zijn op de privacy van persoonsgegevens van medewerkers en/of cliënten vraag je eerst instemming aan de Ondernemingsraad (OR) en/of Cliëntenraad van Amstelring. Ook leg je dit voor aan de privacy officer en functionaris gegevensbescherming.
   Wanneer er bij een locatie camera’s worden ingezet in bijvoorbeeld de gangen en de huiskamer, dan moet dat in overleg met cliëntenraad en de medewerkers moeten geïnformeerd worden.
8. Amstelring stelt voor alle persoonsgegevens die gebruikt worden bewaartermijnen vast en bewaart persoonsgegevens niet langer dan nodig. Amstelring neemt hierbij alle relevante wet- en regelgeving in acht.

   Medisch dossiers worden 20 jaar bewaard, en financiële gegevens 7 jaar. Dit vanwege wettelijke verplichtingen. Als gegevens niet bewaard hoeven te worden, worden ze op correcte wijze verwijderd.

9. Amstelring communiceert begrijpelijk en transparant over het gebruik van persoonsgegevens en informeert betrokkenen over hun rechten bij het gebruik van hun gegevens.

   Op de website van Amstelring is een duidelijke privacyverklaring in te zien.

10. Waar Amstelring samenwerkt met andere partijen neemt Amstelring passende maatregelen om beveiliging en privacy bij deze partijen te waarborgen en legt deze vast in verwerkersovereenkomsten.

    Amstelring tekent met alle leveranciers een verwerkersovereenkomst en controleert of deze voldoet aan de eisen van Amstelring. Met leveranciers, die niet aan deze eisen voldoen, zal niet mee worden samengewerkt.

11. Amstelring verwacht van andere partijen dat zij minimaal hetzelfde privacyniveau handhaven als Amstelring.

    Amstelring controleert in verwerkersovereenkomsten of partijen hetzelfde privacy- en beveiligingsniveau hanteren. Amstelring werkt niet samen met partijen die dat niet kunnen garanderen.

Grondslagen uit de AVG

Amstelring verwerkt alleen persoonsgegevens als er een geldige wettelijke grondslag voor bestaat. De grondslagen uit de AVG zijn:

- **Contract**: het verwerken van persoonsgegevens kan noodzakelijk zijn voor het uitvoeren van een overeenkomst. De meeste zorg bij Amstelring wordt geleverd op grond van een Zorgleveringsovereenkomst met een cliënt of een overeenkomst met een gemeente, verzekeraar of zorgkantoor, etc.
- **Toestemming**: Amstelring maakt, indien nodig, gebruik van geldige toestemming, die transparant wordt omschreven, die actief en ondubbelzinnig gegeven moet worden en welke altijd ingetrokken kan worden. Amstelring gebruikt dit bijvoorbeeld bij gebruik van beeldmateriaal.
- **Gerechtvaardigd belang**: in geval van een gerechtvaardigd belang maakt Amstelring een goede, zorgvuldig gedocumenteerde afweging tussen het organisatiebelang en het belang van de betrokkenen in het kader van de inbreuk op de privacy. Dit gebeurt bijvoorbeeld bij cameratoezicht.
- **Wettelijke plicht**: wanneer er een wettelijke plicht bestaat om gegevens te verwerken, zoals de wettelijke bewaartermijn voor medisch dossiers, dan zal Amstelring daaraan voldoen.
- **Vitaal belang**: in geval van een leven-of-dood situatie mag een arts van Amstelring altijd de persoonsgegevens van een betrokkene verwerken om hem/haar te helpen, na afloop zal hij/zij zich hierover verantwoorden
- **Algemeen belang**: Amstelring zal weinig gebruik maken van deze rechtsgrond.

Inbreuk persoonsgegevens (datalek)

Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een incident dat leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot verwerkte persoonsgegevens, of wanneer niet uitgesloten kan worden dat dit is gebeurd.

Een 'hack' van systemen, waarbij persoonsgegevens worden buitgemaakt, is typisch een voorbeeld van een datalek met kwade opzet.

Er is echter niet altijd sprake van kwade opzet. Een datalek kan per ongeluk optreden, zoals het verliezen van een medisch dossier van een cliënt. Ook wanneer dat dossier later wordt teruggevonden is niet uit te sluiten dat onbevoegden het hebben ingezien. Amstelring wil leren van datalekken en zal steeds zoeken naar manieren om het geleerde te bespreken en continu te verbeteren.

Datalekken moeten altijd gemeld worden bij datalek@amstelring.nl. Meer informatie: Amstelring Datalek Protocol.

Bescherming van privacy van medewerkers

Amstelring beschermt de privacy van de eigen medewerkers goed. Amstelring zal nooit persoonsgegevens van medewerkers delen met andere partijen, tenzij de medewerker daar toestemming voor heeft gegeven, of als er een wettelijke plicht voor bestaat. Amstelring zal nooit zomaar gegevens van de medewerkers delen met derden.

Cameratoezicht

Amstelring maakt in en rondom haar locaties gebruik van cameratoezicht en doet dat door gebruik te maken van de grondslag 'gerechtvaardigd belang'. Cameratoezicht op openbare ruimtes wordt gebruikt om de veiligheid van betreffende ruimtes te waarborgen. Camera's zijn op zo'n manier opgesteld dat zij alleen relevante gebieden voor bescherming van die veiligheid filmen.

Camera's op afdelingen of kamers worden beschouwd als vrijheidsbeperkende maatregelen en zullen altijd in overeenstemming met de Wet Zorg & Dwang worden geïnstalleerd en geëvalueerd. Daar waar gebruik wordt gemaakt van cameratoezicht wordt men geïnformeerd door middel van zichtbare waarschuwingen (bijvoorbeeld een sticker).

Amstelring maakt, tenzij hiervoor zeer zwaarwegende redenen zijn, nooit gebruik van cameratoezicht zonder dat dit bekend is bij de medewerkers of de cliënt (ook wel genoemd heimelijk cameratoezicht). Heimelijk cameratoezicht is alleen

kortdurend toegestaan, en de Raad van Bestuur dient hiervoor een akkoord te geven. Na afloop van heimelijk cameratoezicht zullen alle gefilmde medewerkers en de OR/CCR geïnformeerd worden over het cameragebruik.

Het cameratoezicht aangebracht door familie of cliënten zelf moet uitgeschakeld worden als een medewerker van Amstelring bezwaar heeft tegen het cameratoezicht. Dit moet dus altijd in overleg, zie ook Algemene Voorwaarden Actiz en BTN 2018 algemene module pagina 4 punt 5 onder het kopje 'Welke verplichtingen heeft u'?. Heimelijk installeren van camera's en opnamen maken zonder waarschuwing is bij wet verboden.
Het maken van geluidsopnamen door cliënten of familie van een gesprek met bijvoorbeeld een behandelaar is toegestaan, ook wanneer geen toestemming is gevraagd. De opnamen mogen echter alleen voor eigen gebruik worden benut en niet worden gepubliceerd. Daarnaast is het wettelijk verboden om een gesprek op te nemen waaraan iemand zelf niet deelneemt.

Gedragsregels ICT

De gedragsregels voor het gebruik van ICT-middelen, internet- en e-mailgebruik van Amstelring zijn aanvullend op de algemene gedragsrichtlijn voor medewerkers en vrijwilligers. De Gedragsregels ICT zijn:

- Het is niet toegestaan om ICT-voorzieningen voor onacceptabele persoonlijke doeleinden te gebruiken. Bij onacceptabel persoonlijk gebruik van internet moet onder andere worden gedacht aan: het bezoeken van sites of versturen van berichten die pornografisch, racistisch, discriminerend, dreigend, beledigend of anderszins aanstootgevend materiaal bevatten.
- Het is niet toegestaan om persoonlijke (beeld)informatie van en over cliënten, bezoekers of collega's te plaatsen op social media (Facebook, Linkedin, Twitter, Instagram, Snapchat, etc.) tenzij hiervoor schriftelijk toestemming is gegeven door betreffende perso(o)n(en).
- Beveiligingsincidenten, zoals verdachte of aanstootgevende e-mail moeten gemeld worden aan het ISA. Let ook op phishing-mails (mail die mensen naar een valse websites lokt).
- Het scherm van de computer wordt door de medewerker altijd vergrendeld als de medewerker wegloopt van de computer. Bij een Chromebook volstaat het om de Chromebook dicht te klappen.
- Na het printen van cliënteninformatie, wordt het papier altijd vernietigd. Na het scannen van documenten haalt de medewerker het document uit de scanner en vernietigt het na gebruik. Print alleen indien strikt noodzakelijk.

- Alle gegevens binnen het bedrijfsnetwerk en Google-omgeving zijn van Amstelring.
- Het is niet toegestaan om cliënt-, medewerkers- of bedrijfsinformatie te versturen naar of vanuit je eigen privé e-mailadres.
- Binnen Amstelring zijn ONS, AFAS en Ysis de systemen voor persoons- en medische gegevens en deze gegevens hoeven niet meer intern gemaild te worden. Mocht er toch noodzaak zijn tot mailen van persoonsgegevens, dan is het niet toegestaan om dit naar groepsmailboxen of distributielijsten (mailgroepen) te mailen (maar alleen naar individuele e-mailadressen van personen).

Verder is de gedragsrichtlijn medewerkers en vrijwilligers van kracht. Hierin staan ook enkele zaken opgenomen die te maken hebben met privacy.

Toegang tot systemen

De NEN normen (7510 e.v.) gelden voor zorgorganisaties maar past Amstelring op vergelijkbare wijze toe voor personeels en andere informatie, afhankelijk van de gevoeligheid daarvan.

Wat zijn autorisaties en toegang

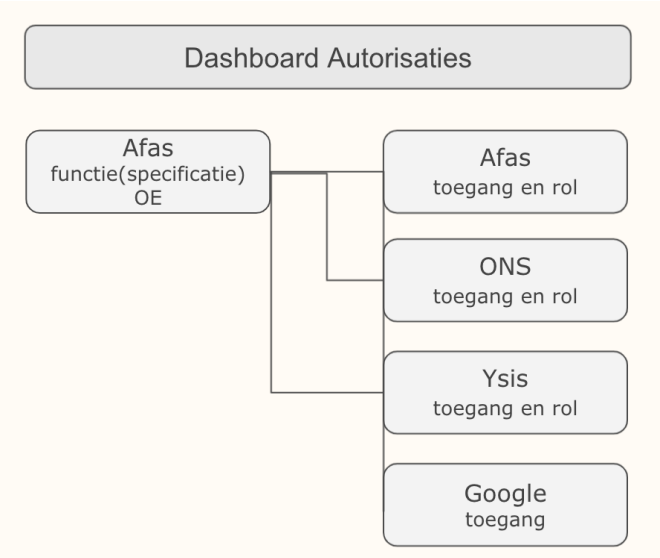
Autorisatie gaat over wat iemand mag, en welke informatie iemand mag zien en bewerken binnen een systeem. *Toegang* gaat over voor welke medewerkers een autorisatie geldt. Voor iedere applicatie wordt een 'autorisatiematrix' opgesteld door de proceseigenaar en de applicatiebeheerder. Indien wordt afgeweken van de uitgangspunten, documenteren we waarom en leggen we de afwijking voor aan de stuurgroep Informatieveiligheid (bijvoorbeeld 'niet mogelijk in de applicatie' of 'wens proceseigenaar'). Door deze werkwijze:

- kunnen autorisatie vraagstukken worden opgelost;
- is het mogelijk om medewerkers eenduidig te autoriseren;
- is de informatiebeveiliging van Amstelring -voor dit onderwerp- aantoonbaar;
- borgen we de kwaliteit van gegevens.

Amstelring kent een aantal kernprocessen, zoals personeel, zorgverlening, financiën en dergelijke. Bij deze kernprocessen horen informatieverwerkende systemen. Zo wordt het kernproces personeel verwerkt in AFAS, het zorgproces in ONS en Ysis, etc. Deze systemen worden door een specifieke groep gebruikers gebruikt en door een groep medewerkers beheerd en ondersteund.

Introductie van rolspecifieke expertise

Binnen deze systemen zijn rollen toebedeeld op basis waarvan bevoegdheden en toegangsrechten eenduidig worden toegekend. De registratie van de functie (-specificatie) in AFAS is leidend. De inhoud van de rollen ligt vast in de autorisatiematrix. Daarin is ook aangeduid welke rollen als kritisch (niet verenigbaar) worden beschouwd. NB: het gaat hier om de functionele beschrijving. In AFAS wordt een veld toegevoegd waarin rolspecifieke expertise wordt vastgelegd mede op basis waarvan bepaald wordt welke autorisaties een medewerker krijgt. in die zin heeft Afas een dubbele functie: bepaalt welke autorisaties iemand mag krijgen op basis van functie (-expertise) en organisatie plek en daarnaast moeten de rollen binnen Afas ook afgezet worden tegen Afas. Zie hiervoor het volgende overzicht:



Medewerkers (al dan niet intern, dus ook de uitzendkrachten, flexwerkers) maar ook leveranciers, cliënten etc. krijgen rollen toebedeeld. Als voor specifieke functies bepaalde verzamelingen van rollen bestaan kunnen deze functies als aggregatie van rollen worden gehanteerd. Dus medewerkers krijgen rollen toebedeeld, afhankelijk van hun functie en de aard van hun werkzaamheden.

Aan deze rollen worden vervolgens rechten toegekend. Deze rechten worden in eerste instantie in algemene zin geformuleerd zodat duidelijk is wat de bedoeling van de rol is.
Bijvoorbeeld het verwerken van cliënten in de administratie van Amstelring. Daaronder wordt verstaan het aanmelden van nieuwe cliënten, het wijzigen van gegevens van deze cliënten en het uitschrijven van cliënten. Vervolgens wordt gekeken welke specifieke bevoegdheden daarbij horen in de daarvoor binnen Amstelring gebruikte systemen.

Uitgangspunten autorisaties en toegang

Bij het opstellen van de uitgangspunten voor autorisatie en toegang hanteren we het onderstaande beleid:

- Betrouwbare informatie is alleen te verkrijgen door medewerkers die goed getraind zijn in de functionaliteiten van de applicaties, zodat ze deze goed en

veilig gebruiken.

- Alle informatie nodig om het werk te kunnen doen: medewerkers moeten toegang hebben tot alle informatie die ze nodig hebben om hun werkzaamheden te kunnen verrichten.
- Functiescheiding: stappen in een proces worden - daar waar het privacy of andere risico's kent - opgesplitst tussen medewerkers, functiegroepen en systemen.
- 1 keer vastleggen door te registreren bij de bron en te faciliteren met slimme ICT. Hierbij ligt de verantwoordelijkheid bij de medewerker.
- Waar toegangscontroles onvoldoende de risico's afdekken wordt dit aangevuld met signaallijsten (datagedreven controle) of andere aanvullende maatregelen. De controles worden opgenomen in de procesbeschrijvingen.
- **Admin** rechten in een applicatie zijn altijd voorbehouden aan een zeer beperkt aantal, zeer deskundige medewerkers: de applicatiebeheerders en zijn altijd op naam. Admin rechten gaan boven wijzigingen op individueel cliënt/medewerker niveau, zoals bijvoorbeeld wijzigingen in master data[1] in opdracht van bijvoorbeeld bedrijfsinformatie of zorginkoop, autorisaties aanpassen binnen de kaders van de opgestelde autorisatiematrices, configureren, koppelingen aanpassen, etc. De admin accounts moeten worden toegewezen aan een applicatiebeheerder. Dan is herleidbaar wie welke admin account heeft gebruikt. Vb: admin1 = applicatiebeheerder 1 etc. Een andere optie is gebruik te maken van een logboek.
- Om te controleren of er niet een te ruime autorisatie wordt toegekend aan gebruikers, wordt in Tableau overzichten getoond waaruit blijkt waar dit beleid goed en niet goed wordt uitgevoerd.
- Als er naast de functioneel applicatiebeheerder nog andere gebruikers zijn die stamtabellen kunnen wijzigen, moet er een rapportage zijn die deze wijzigingen inzichtelijk maakt.
- Wanneer de rechtenstructuur binnen een applicatie niet fijnmazig genoeg is om een medewerker exact de juiste autorisatie te geven, kiest Amstelring voor het verstrekken van rechten die zo dicht mogelijk in de buurt komen van wat de medewerker nodig heeft. Tegelijk blijft Amstelring de leverancier aansporen om aanpassingen in de applicatie aan te brengen.
- Een medewerker die - door de beperkingen in de autorisatie-mogelijkheden van een applicatie - meer autorisaties krijgt dan nodig is voor de werkzaamheden, wordt uitvoerig getraind zodat helder is welke functies niet gebruikt mogen worden en welke gevolgen het heeft als de medewerker dit toch doet.
- De juiste autorisaties voor gebruik van persoonsgegevens zijn geregeld in de primaire applicaties, bijvoorbeeld Ons, Afas en Puur. Autorisaties binnen overige applicaties of reporting-tools die gebruik maken van de persoonsgegevens uit

[1] Master data: kostenplaatsen, nieuwe producten, afdelingen, etc.

deze applicaties, inclusief het downloaden, gebruiken en delen van informatie uit deze applicaties naar bijvoorbeeld Spreadsheets of Excel, mogen nooit verder gaan qua inzage in persoonsgegevens dan geregeld in de primaire applicaties. Afwijkingen hierop kunnen aangevraagd worden via informatieveiligheid@amstelring.nl.

- Informatie over een cliënt is alleen zichtbaar voor een medewerker indien de medewerker een behandelrelatie heeft met de cliënt.
- Artsen hebben een bredere toegang. Een arts kan ook informatie zien van cliënten waar hij/zij geen directe behandelrelatie mee heeft. Artsen nemen diensten voor elkaar waar en hebben daarom een bredere toegang tot cliëntgegevens nodig.
- Informatie over een medewerker is zichtbaar voor een andere medewerker wanneer dit nodig is voor de werkzaamheden die bij zijn of haar rol horen. Zo kan bijvoorbeeld een roosteraar het deskundigheidsniveau van iemand inzien omdat dit nodig is bij het roosteren. Een salarisadministrateur kan de salarissen van iedereen inzien.
- Wanneer medewerkers problemen ervaren met een account (of applicatie), zoals onvoldoende autorisatie of toegang, nemen ze contact op met het ISA.
- Amstelring maakt **geen groepsaccount** aan wanneer met het groepsaccount persoonsgegevens bewerkt of ingezien kunnen worden.
- Groepsmailboxen zijn toegestaan. Persoonsgevoelige gegevens worden niet gemaild naar groepsmailboxen. Groepsmailboxen worden altijd vanuit een persoonlijk account benaderd.
- Voor het vervangen van een collega, bijvoorbeeld tijdens verzuim of verlof, worden tijdelijk extra rechten toegekend volgens een vaste afspraak (die is vastgelegd bij de autorisatiematrix).

In deze procesbeschrijving wordt het proces van autorisaties en toegang beschreven.

Functiescheiding en rollen

Bij functiescheiding onderkent Amstelring twee belangrijke risico's:

1. Ongeautoriseerde mutaties (fouten)
2. Onbedoelde toegang tot (privacy)gevoelige informatie

Om het risico op het voordoen van deze risico's te mitigeren, zijn er twee zaken van belang. Vastgesteld en vastgelegd moet worden:

Wie mag wat muteren?
Wie mag wat zien?

Daarnaast dienen geregeld samenhangende controles te worden uitgevoerd. Daarbij wordt het principe van functiescheiding gehanteerd. Bijvoorbeeld de medewerker FA controleert mutaties in crediteurenstamgegevens aan de hand van mutatieverslag. Alleen inkoop muteert crediteurenstamgegevens.

DUS

Applicatiebeheer

- functiescheiding tussen applicatiebeheer en medewerkers
- applicatiebeheerders mogen geen transacties doorvoeren
- zichtbare periodieke controle op toegekende rechten

Superusers

- Let bij invoer van stamgegevens (inrichting: bijvoorbeeld producten / tabelgegevens grootboekrekeningen, kostenplaatsen) ook op zichtbare controles in functiescheiding.

Inkoop tot betalen-proces (AFAS/Proquro/Internetbankieren):

- Scheiding tussen vastleggen van de inkoop (verplichting) en de autorisatie (conform procuratieregeling)
- Scheiding tussen muteren van crediteurenstamgegevens en de financiële administratie (invoercontrole);
- Scheiding tussen het fiatteren van inkoopfacturen/bestellingen en de financiële administratie;
- Scheiding tussen het aanmaken van de betaaladvieslijst en de controle daarop;
- Scheiding tussen 1e en 2e handtekening in de bankapplicatie.

Indienst- mutaties - uitdienst proces (medewerkers, externen, vrijwilligers)

- Scheiding tussen registratie indiensttreding / mutatie / uitdienstmelding en autorisatie door leidinggevende.
- Input HR adviseur in workflow (m.b.t. CAO / salaris toekenning)
- Scheiding tussen aanmaken mutatie in Afas, autoriseren daarvan en de verwerking;
- Scheiding tussen aanmaken mutatie en de controle daarvan.

Declaraties

- Scheiding tussen declarant en controleur (steekproefsgewijs)
- Proces mogelijk in Afas?

HRM: personeelsdossier

- Classificatie: gradaties van vertrouwelijkheid
    - Muteren personeelsdossier alleen door HR adviseur
    - Inzage personeelsdossier directe leidinggevende en (welke onderdelen?)
    - (Tijdelijke) inzage personeelsdossier door leidinggevende …..
    - Verzuimdossier door verzuimspecialist

Debiteuren

- Scheiding tussen incasso en administratie

Testomgeving

- Amstelring heeft een aantal Afas testomgevingen

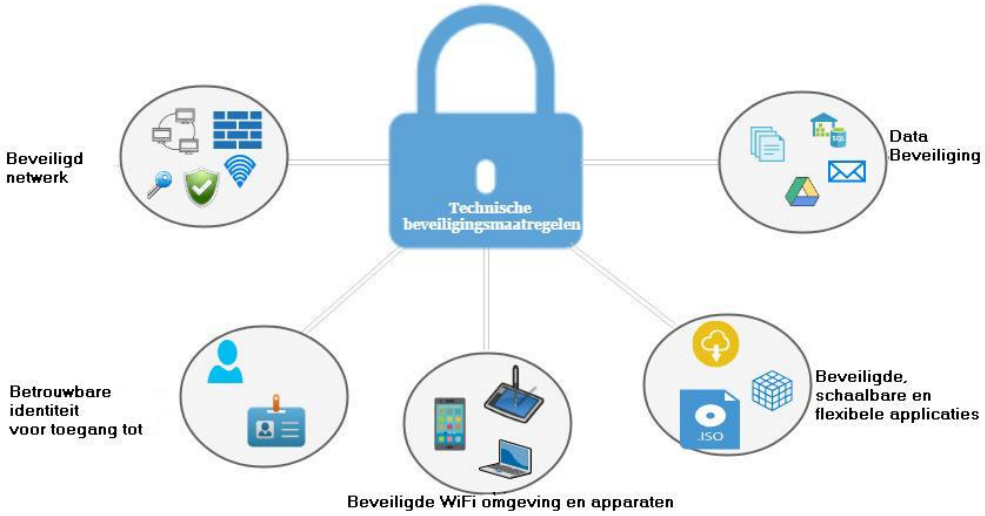
Zorgproces (ONS/NEDAP):

- De scheiding tussen indicatie stellen (niveau 5 verpleegkundige) en het plannen enerzijds en uitvoeren anderzijds;
- de scheiding tussen uitvoeren en fiatteren;
- de scheiding tussen registreren en controleren.

Hoe zorgen we dat alles blijft werken

Technische maatregelen

Technische maatregelen worden ingezet om op een veilige wijze data te verwerken. Een netwerk zonder beveiliging is immers als een huis zonder slot op de voordeur. De beveiliging van het netwerk begint bij de ingang die toegang verschaft tot alle systemen, waarbij rekening gehouden wordt met het soort apparaten dat tegenwoordig op de werkvloer worden gebruikt.



Binnen Amstelring zijn de systemen berekend op **één ramp tegelijk.** Zo kan er omgegaan worden met stroomuitval, waterschade, brand of zombies, maar niet alle 'rampen' tegelijk. Onderstaand een aantal technische maatregelen die ingezet worden:

- **Beveiligd netwerk:** Er zijn diverse maatregelen genomen om het Amstelring computernetwerk te beveiligen tegen ongeautoriseerde toegang. Antivirus, spamfilters, Firewalls, wachtwoordbeleid, twee stappen authenticatie, data encryptie, LAN scheiding (gescheiden netwerken) en radius authenticatie zijn hier onderdeel van.

- **Gecontroleerde identiteit geeft toegang tot:** Het gaat hier primair om de authenticatie en de toegangsrechten die een gebruiker heeft in het netwerk, de zogenoemde autorisatie. Er wordt op toegezien dat de juiste personen de juiste rechten hebben en dat hier geen misbruik van gemaakt wordt.

- **Beveiligde WiFi omgeving**: Het WiFi netwerk is een gescheiden omgeving welke is opgedeeld in een aantal netwerken waarbij, met uitzondering van het gastennetwerk, beveiligingsmethodes zijn ingesteld.

- **Beveiligde, schaalbare en flexibele applicaties:** SaaS (Software as a Service) applicaties en SSO (single sign on) worden ingezet waardoor beschikbaarheid, schaalbaarheid en stabiliteit fors worden vergroot.

- **Data beveiliging:** Naast organisatorische maatregelen worden door de bovenstaande maatregelen datalekken en onbevoegde toegang tot bedrijfsinformatie voorkomen. Kwetsbaarheden in het netwerk proberen we op te sporen door jaarlijks een Pentest uit te voeren.

- **Wachtwoordbeleid:** Een wachtwoordbeleid wordt ingesteld om te voorkomen dat er misbruik wordt gemaakt van de toegang tot een digitale omgeving en data. Het beleid is meer dan alleen een aantal eisen.
  Naast complexe wachtwoorden, 2 stappen authenticatie en controle op het aantal inlogpogingen traint Amstelring ook op bewustwording en het belang van informatiebeveiliging in trainingen/cursussen.

- **Apparaten**: De mobiele apparaten van Amstelring worden zoveel mogelijk individueel uitgegeven. Een uitzondering hierop zijn de team telefoons. De registratie hiervan is in Afas. Er is hier apart beleid voor vastgesteld. Voor de (externe) medewerker is het toegestaan om een apparaat dat niet beheerd wordt door Amstelring te gebruiken voor applicaties waar de toegang goed is geregeld (2FA, NEN-gecertificeerd). Een uitzondering hierop zijn bijzondere toegang tot ons netwerk, zoals bijvoorbeeld het gebruik van VPN-verbindingen. Hiervoor is een ‘trusted device’ verplicht.
  De bedrijfsapparaten (smartphones, ipads, en chromebooks) worden middels een Mobile Device Management systeem beheerd.

Leveranciersmanagement

Doordat cloud-applicaties worden ingezet is het minder duidelijk waar applicaties en gegevens zich feitelijk bevinden. Strenge afspraken met leveranciers over beveiliging (oa. ISO- en NEN-normen) en verantwoordelijkheid zijn belangrijk. Dit wordt vastgelegd in Service Level Agreements en wanneer in de applicaties persoonsgegevens verwerkt worden ;verwerkers-overeenkomsten. In de verwerkersovereenkomst wordt geregeld hoe de leverancier dient om te gaan met de persoonsgegevens. Om er zeker van te zijn dat de leveranciers voldoen aan de afspraken, vragen wij jaarlijks ISAE 3402 type II rapportages op. Daarnaast vragen wij om een ISO-certificering en aanvullend of wordt voldaan aan de NEN-normen. Wanneer dit niet het geval is wordt gezocht naar manieren om erachter te komen of een leverancier de zaken goed heeft geregeld. Als blijkt dat dit niet het geval is of

de leverancier niet op korte termijn wel zijn zaken op orde kan krijgen, wordt niet met de betreffende leverancier gewerkt.
Amstelring wil ontzorgd worden door leveranciers maar ook altijd de regie blijven houden. De SLA is hierop aangepast, ook is transparantie en rapportages over security-incidenten een apart onderdeel van de SLA.

Continuïteitsplan

Om de beschikbaarheid van de vitale bedrijfsprocessen en informatievoorziening onder normale en buitengewone omstandigheden te waarborgen, zijn enkele processtappen en activiteiten nodig. In het Continuïteitsplan wordt dit beschreven. Amstelring zorgt voor iedere calamiteit in de it-omgeving voor een alternatief. Er wordt derhalve niet voorzien in gelijktijdige calamiteiten.

Risico Impact Assessment (RIA)

Als jij of je team besluit om nieuwe IT systemen of processen te gebruiken, bestaande systemen of processen aan te passen (of stop te zetten) moeten de **privacy, beveiliging en IT risico's** in kaart worden gebracht en eventueel risicoverlagende maatregelen genomen worden voordat de wijzigingen gemaakt worden.
Het in kaart brengen van de risico's en het bedenken van risico verlagende maatregelen is mogelijk met behulp van de Amstelring Risico Impact Assessment (hierna: **RIA). RIA's bestaan uit een vragenlijst die door een initiatiefnemer moet worden ingevuld. Dit assessment start met een aantal situatie vragen zodat snel duidelijk word**t of er een kort assessment (laag risico) of uitvoerig assessment (hoog risico) nodig is. **Mocht de initiatiefnemer hulp nodig hebben bij het invullen, kan hij/zij ondersteunin**g vragen aan de regiehouder IT, adviseurs op gebied van digitalisering of met de security consultant of FG via informatieveiligheid@amstelring.nl.
Het resultaat van het assessment (de antwoorden op de vragen) wordt gedeeld met de functionaris gegevensbescherming en/of stuurgroep informatieveiligheid, wat kan leiden tot aanvullende privacy- en/of beveiligingsmaatregelen, het ongewijzigd doorvoeren van de wijziging of het niet doorvoeren van de wijziging.
Hier is een link naar het formulier. Vul dit altijd in als je met een nieuwe wijziging bezig bent.

Links

procedure datalekken
privacyverklaring
website Amstelring
Autoriteit persoonsgegevens
NEN 7510