ZIEKENHUIS
ST ANTONIUS

Beleid gegevensbescherming en informatiebeveiliging

Het St. Antonius Ziekenhuis beschermt persoonsgegevens en de continuïteit van patiëntenzorg.

Colofon
Datum: 28-11-2024
Informatie classificatie: publiek
Eindredactie: Corporate Information Security Officer
Goedkeuring: RvB

Inhoudsopgave

1. Algemeen

1.1. Inleiding

Als zorginstelling is het St. Antonius Ziekenhuis verantwoordelijk voor patiëntenzorg, onderzoek en onderwijs. Het leveren van kwaliteit staat bij het uitvoeren van deze taak voorop. Om deze kwaliteit aan de patiënten en andere betrokkenen te kunnen bieden is een betrouwbare informatievoorziening essentieel. Informatie moet alleen toegankelijk zijn voor geautoriseerde personen, correct zijn en altijd beschikbaar zijn wanneer nodig.

Dit beleid 'Gegevensbescherming en Informatiebeveiliging' geeft richtlijnen om aan deze vereisten te voldoen.

Leeswijzer

In het vervolg van dit hoofdstuk worden de begrippen privacy, gegevensbescherming en informatiebeveiliging nader gedefinieerd en wordt de reikwijdte van het beleid toegelicht. Hoofdstuk 2 beschrijft de wet- en regelgeving waardoor ons beleid wordt omkaderd. Hoofdstuk 3 beschrijft ons beleid. In hoofdstuk 4 wordt de vertaling van het beleid naar onze ziekenhuisorganisatie beschreven. In hoofdstuk 5 is de governance, zoals rollen en verantwoordelijkheden, toegelicht. Nadere achtergrondinformatie is opgenomen in bijlagen.

1.2. Privacy en gegevensbescherming

Privacy gaat om de bescherming van persoonsgegevens; de bescherming van het eigen lichaam en van de eigen woning; de bescherming van familie- en gezinsleven en het recht vertrouwelijk te communiceren via brief, telefoon en e-mail. Privacy betekent dat iemand dingen kan doen zonder dat de buitenwereld daar weet van heeft, inbreuk op maakt, of een corrigerende invloed op uitoefent.

Het is belangrijk dat onze patiënten erop kunnen vertrouwen dat we zorgvuldig omgaan met hun persoonsgegevens. Patiënten bevinden zich immers in een kwetsbare en afhankelijke situatie. Dat geldt zeker voor kinderen, mensen die ernstig ziek zijn of voor ouderen met een kwetsbare gezondheid. Ze hebben onze zorg nodig en kunnen zich onzeker voelen over hun gezondheidssituatie. Een situatie die ze niet altijd willen delen met anderen. Het beroepsgeheim en de AVG brengen dan ook belangrijke plichten met zich mee voor elke zorgverlener en medewerker die persoonsgegevens verwerkt.

Gegevensbescherming is het samenstel van wetgeving, beleidsregels, standaarden en normen waarin technische en/of organisatorische maatregelen worden beschreven ter bescherming van de persoonsgegevens van patiënten en medewerkers. Onder medewerkers worden niet alleen de werknemers die een dienstverband met het St. Antonius Ziekenhuis hebben bedoeld, maar ook zij die zonder dienstverband voor of namens het St. Antonius hun diensten aanbieden en onder het gezag van de organisatie vallen.

In dit beleidsdocument ligt de focus voor privacy en gegevensbescherming op de verschillende onderdelen van de uitvoering van de Algemene Verordening Gegevensbescherming (AVG). Het is belangrijk dat medewerkers zich ervan bewust zijn dat het werken met persoonsgegevens een grote verantwoordelijkheid met zich meebrengt.

Dit beleidsdocument geeft aan hoe we binnen het St. Antonius Ziekenhuis omgaan met gegevensverwerkingen en gegevensbescherming en hoe we een en ander intern hebben georganiseerd. Hiermee geeft het St. Antonius Ziekenhuis invulling aan haar verantwoordingsplicht op grond van de Algemene Verordening Gegevensbescherming (AVG). Het biedt het kader waarbinnen medewerkers op verantwoorde en zorgvuldige wijze persoonsgegevens kunnen verwerken. Dit document moet tevens worden gezien als raamwerk voor (nader uit te werken) specifieke beleidsstukken en procedures. Die uitwerkingen mogen niet strijdig zijn met ons hoofdbeleid. In de bijlage verwijzen we naar de reeds beschikbare uitwerkingen.

In dit beleidsdocument hanteren we voor gegevensbescherming de volgende begrippen en definities:

Begrip	Definitie
Anonieme gegevens	Gegevens die door niemand en op geen enkele wijze meer tot een natuurlijk persoon te herleiden zijn.
Pseudonieme gegevens	Gegevens die indirect tot een natuurlijk persoon te herleiden zijn (bijvoorbeeld door codering), ook als dit niet eenvoudig is uit te voeren.
Betrokkene	Geïdentificeerde of te identificeren natuurlijke persoon op wie de gegevensverwerking betrekking heeft.
Verantwoordelijke	St. Antonius Ziekenhuis, vertegenwoordigd door de RvB.
Datalek	Elke inbreuk op de beveiliging van persoonsgegevens die per ongeluk of onrechtmatig leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking of toegang tot verwerkte gegevens.
Intern verantwoordelijke	Elke medewerker die ten behoeve van het ziekenhuis het doel en de middelen bepaalt voor een gegevensverwerking.
Verwerken	Elke handeling (bewerking) met persoonsgegevens (al dan niet via automatische procedés), zoals verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, wissen en vernietigen.
Verwerker	Een rechtspersoon of natuurlijk persoon die in opdracht van of ten behoeve van de Verantwoordelijke persoonsgegevens verwerkt. De gegevensverwerking is de primaire opdracht (in tegenstelling tot het verlenen van een andere dienstverlening).

1.3. Informatiebeveiliging

Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Het doel is het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie(voorziening) en het beperken van de gevolgen van eventuele beveiligingsincidenten.

In dit beleidsdocument ligt de nadruk voor informatiebeveiliging op het beleggen van de verantwoordelijkheden volgens de NEN 7510 norm. Deze norm is de standaard voor informatiebeveiliging in de zorg (zie ook paragraaf 2.3).

1.4. Reikwijdte

Personen, locaties

Het beleid is van toepassing op de gehele organisatie van het St. Antonius Ziekenhuis, op alle locaties en op iedereen die er werkzaam is. Indien medewerkers van maatschappen of externen gebruik maken van diensten van de organisatie is het beleid automatisch ook op hen van toepassing.

Gegevens

Dit beleidsdocument is van toepassing op alle verwerkingen van persoonsgegevens waarvoor het St. Antonius Ziekenhuis verantwoordelijk is. Dit betreft alle verwerkingen door medewerkers, artsen of derden die voor onze dienstverlening worden ingezet (zowel bedrijven als Personeel Niet In Loondienst) en voor alle vestigingen van het ziekenhuis. Dit geldt dus ook voor het Coöperatief Medisch Specialistisch Bedrijf en de daarvoor werkzame artsen en medewerkers. De verwerkingen betreffen niet alleen patiëntgegevens, maar ook persoonsgegevens van medewerkers, bezoekers, patiëntvertegenwoordigers en andere derden.
NB: indien volstrekt anonieme gegevens worden verwerkt, is de AVG niet van toepassing en hoeft niet aan alle voorwaarden in dit document te worden voldaan. Of er sprake is van anonieme gegevens moet zorgvuldig te worden beoordeeld. Op gepseudonimiseerde gegevens is dit document volledig van toepassing. De reikwijdte van ons beleid wordt tot slot mede gevormd door het wettelijk kader dat in hoofdstuk 2 is toegelicht.

2. Wettelijk kader

Wet- en regelgeving vereist van onze organisatie dat iedereen in onze organisatie volgens bepaalde richtlijnen met vertrouwelijke (persoons)gegevens omgaat, in het bijzonder wanneer deze gegevens uitgewisseld worden met ontvangers buiten onze organisatie. In dit hoofdstuk lichten we drie belangrijke onderdelen van het wettelijk kader uit.

2.1. De Algemene Verordening Gegevensbescherming (AVG)

De EU heeft, in navolging van de Europese Richtlijn van 1995, besloten om de Europese privacywetgeving aan te passen aan het huidige digitale tijdperk en dit op strikte wijze afdwingbaar te maken middels de Algemene Verordening Gegevensbescherming (AVG). De AVG regelt dat het hele proces van gegevensverwerking, van het verzamelen tot het vastleggen, doorgeven en vernietigen van persoonsgegevens aan zorgvuldigheidseisen moet voldoen. Het gaat dan om alle gegevens die tot de persoon herleidbaar zijn, waaronder ook patiëntgegevens.
Het St. Antonius Ziekenhuis geeft inhoud aan deze verordening en de Uitvoeringswet AVG door het opstellen van regels en richtlijnen waaraan ieder die in het ziekenhuis werkt zich moet houden. Het St. Antonius Ziekenhuis hecht er grote waarde aan dat patiënten, medewerkers en verwijzers erop kunnen vertrouwen dat gegevens bij ons in veilige handen zijn. Ook gaan de strenge eisen van de AVG gepaard met hoge boetes in geval van overtreding hiervan.

Rol Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens (AP) houdt in Nederland toezicht op de naleving van de AVG. Zij heeft daarnaast een aantal hulpmiddelen aangereikt om op gestructureerde wijze te voldoen aan de AVG. De nadruk ligt hierbij op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden. Zo is het St. Antonius Ziekenhuis verplicht een functionaris gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen het ziekenhuis toezicht houdt op de toepassing en naleving van de AVG en een rechtstreekse communicatielijn naar de RvB heeft.

Rechten en plichten
Enerzijds versterkt de AVG de positie van mensen van wie gegevens worden verwerkt. Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Anderzijds krijgen organisaties die persoonsgegevens verwerken meer verplichtingen. Zo verplicht de AVG ons dat we de gegevens die wij (of anderen voor ons) verwerken, contractueel vastleggen in een **verwerkersovereenkomst** en registreren in een **verwerkingenregister**. Daarom brengen we voordat we nieuwe apparatuur installeren of samenwerkingsverbanden aangaan, eerst in kaart welke gevolgen dat heeft voor het verwerken van persoonsgegevens.
Als persoonsgegevens verloren gaan of onbevoegd worden ingezien, moeten we hier transparant en open over communiceren naar zowel de toezichthouder als de gedupeerde.

Maatregelen
Belangrijk criterium bij de handhaving van de AVG is dat organisaties - binnen redelijke grenzen - alle organisatorische en technische maatregelen dienen te nemen om de persoonsgegevens van natuurlijke personen te beschermen. Dit om de privacybelangen van patiënten, medewerkers en andere betrokkenen te beschermen op aantoonbare, verantwoorde en controleerbare wijze. Er dienen tevens verbetercycli en -mechanismen aanwezig te zijn.
In geval van verwerkingen, die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen, moet een Data Protection Impact Assessment (DPIA)[1] uitgevoerd te worden. DPIAs behoren voorafgaand aan ingebruikneming plaats te vinden.
In geval van bestaande verwerkingen moet een DPIA plaats te vinden:
- Wanneer deze nog niet is uitgevoerd;
- Bij introductie van een nieuwe technologie of applicatie of leverancier;
- Indien persoonsgegevens voor een ander doel gebruikt gaan worden.

[1] Een DPIA brengt de risico's van een gegevensverwerking in kaart om daarna maatregelen te kunnen nemen om deze risico's te verkleinen.

2.2. De Wet kwaliteit, klachten en geschillen zorg (Wkkgz)

De overheid vereist dat iedereen goede zorg krijgt. De overheid heeft wettelijk vastgelegd wat goede zorg precies inhoudt en wat er moet gebeuren als mensen een klacht hebben over de zorg. Het kader hiervoor is de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en het Uitvoeringsbesluit Wkkgz.

De rol van de IGJ

De IGJ houdt onder meer vanuit de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) toezicht op het St. Antonius Ziekenhuis. De IGJ kijkt ook naar de toepassing van e-health door zorgaanbieders. Hiervoor is een apart toetsingskader opgezet. Ook specifieke eisen vanuit de NEN 7510 norm zijn hierin opgenomen. Immers goede zorg is grotendeels afhankelijk van een goed functionerende ICT voorziening.

2.3. De NEN 7510 norm

Om de zorgsector handvaten te geven voor het inrichten van informatiebeveiliging is de norm NEN 7510 opgesteld. Deze Nederlandse norm voor informatiebeveiliging in de zorg is gebaseerd op de internationale norm ISO 27001, waaraan we ook voldoen voor onze internationale connecties. Deze normen geven een praktisch kader om informatiebeveiliging te organiseren. De risicogerichte benadering van deze normen zorgen ervoor dat we beveiligingsrisico's identificeren en op gestructureerde wijze aanpakken. Door implementatie van deze normen verminderen we de kans op beveiligingsincidenten en de ernst ervan. De IGJ hanteert zoals eerder vermeld de NEN 7510 in haar toetsingskader.[2]

De NEN 7510 norm dekt het hele gebied van informatiebeveiliging en blijft dus niet beperkt tot technische specificaties maar geeft ook richting aan de organisatie en het menselijk handelen. De norm is verder van toepassing op zowel geautomatiseerde als niet geautomatiseerde informatie. De NEN 7510 omvat vereisten voor naleving van (overige) wettelijke en contractuele eisen. Ook bevat de NEN 7510 de best practices op het gebied van informatiebeveiliging, inclusief maatregelen voor versleuteling van gegevens die expliciet in de AVG vermeldt staat. De NEN 7510 vereist het borgen van naleving van wettelijke en contractuele eisen inclusief de AVG. Omgekeerd vereist de AVG de toepassing van passende technische en organisatorische maatregelen voor gegevensbescherming. In die zin sluiten de eisen van de AVG en de maatregelen uit de NEN 7510 norm naadloos op elkaar aan. De NEN 7510 is daarom hét kader voor informatiebeveiliging in het St. Antonius Ziekenhuis. Door certificering en het laten uitvoeren van audits is geborgd dat het St. Antonius Ziekenhuis aan deze norm voldoet.

2.4. De Network and Information Security directive (NIS-2 richtlijn)

Deze Europese richtlijn is opgesteld om risico's die netwerk- en informatiesystemen bedreigen te beheersen wanneer deze een ernstig verstorend effect kunnen hebben voor de samenleving. De NIS-2 is de opvolger van de eerste NIS-richtlijn, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) maar is op meer sectoren en organisaties van toepassing. De NIS-2 kent drie onderdelen:

1. Zorgplicht: Organisaties moeten voldoende maatregelen treffen om zichzelf te beschermen.
2. Meldplicht: Ernstige incidenten moeten binnen 24 uur gemeld worden bij een toezichthouder (nog niet vastgesteld voor Nederland).
3. Toezicht: Per land komen één of meerdere toezichthouders.

Onbekend is nog hoe deze richtlijn concreet vertaald zal worden naar Nederlandse wet- en regelgeving. Naar verwachting moet het St. Antonius Ziekenhuis eind 2025 hieraan voldoen. De IGJ wordt toezichthouder voor de zorgsector.

2.5. Overige wet- en regelgeving

Overige relevante wet- en regelgeving (niet nader toegelicht) zijn:

- Wet geneeskundige behandelingsovereenkomst (WGBO met aanvullende zorgwetgeving);
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wet gebruik burgerservicenummer in de zorg, en regels omtrent elektronische verwerking van gegevens);
- Wet elektronische gegevensuitwisseling in de zorg (Wegiz);

[2] De NEN 7510 is ook opgenomen in het Besluit elektronische gegevensverwerking door zorgaanbieders.

- Wet medisch-wetenschappelijk onderzoek met mensen (WMO);
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG);
- MDR verordening (inzake medische hulpmiddelen);
- AI Act (inzake kunstmatige intelligentie)[3];
- European Health Data Space (EHDS - juridisch kader voor gebruik gegevens voor gezondheid, zowel primair als secundair gebruik).[4]

[3] Deze verordening is sinds augustus 2024 in werking getreden en is 2 jaar later volledig van toepassing. Uitzonderingen: verbodsbepalingen worden na 6 maanden van kracht, governance regels en verplichtingen voor AI-modellen voor algemene doeleinden na 12 maanden en de regels voor AI-systemen (ingebed in gereguleerde producten) na 36 maanden.
[4] Politiek akkoord in maart 2024 bereikt. Vereist ook aanpassing van Nederlandse wetgeving i.v.m. invoering opt-out systeem.

3. Het beleid

3.1. Missie, visie

Missie
Voor het St. Antonius Ziekenhuis is de volgende missie geformuleerd: **"Het St. Antonius Ziekenhuis beschermt persoonsgegevens en de continuïteit van patiëntenzorg."**

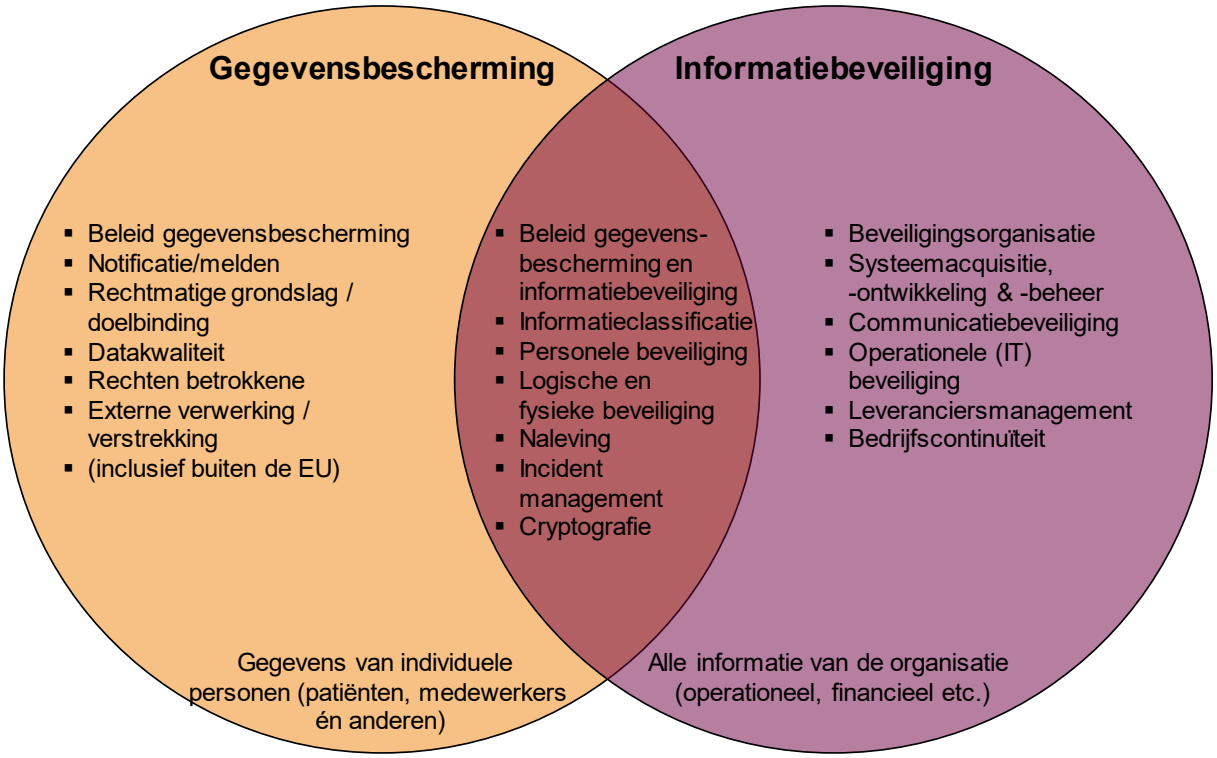
Dit betekent dat we zorgvuldig omgaan met de gegevens van patiënten medewerkers en andere betrokkenen en tegelijkertijd zorgdragen dat de continuïteit van de patiëntenzorg gewaarborgd is, ook bij de uitval van ICT systemen.

Visie
Het St. Antonius Ziekenhuis kent de kernwaarden **Samen, Betrokken, Continu verbeteren en Innovatie**.
Professionele informatiebeveiliging is essentieel bij het uitdragen van deze kernwaarden. We werken steeds vaker (multidisciplinair) **samen** waardoor we meer informatie met elkaar uitwisselen. **Betrokken** medewerkers vereist dat zij kunnen rekenen op een goede informatievoorziening. Als ambitieus ziekenhuis dat **continu** wil **verbeteren**, moeten we continu kunnen beschikken over de juiste informatie. Bovendien vraagt de enorme snelheid van **innovatie** van ons dat we de juiste informatie kunnen inzetten om hierin voorop te kunnen blijven lopen. Een belangrijke randvoorwaarde voor het gebruik van informatie is de bescherming ervan.

Zorgvuldige afwegen van belangen
Gegevensbescherming en informatiebeveiliging zijn een integraal onderdeel van patiëntenzorg: als de beschikbaarheid, integriteit en vertrouwelijkheid van informatie niet geborgd zijn is het leveren van zorg niet goed meer mogelijk. Toch kunnen in bepaalde situaties de kwaliteit van zorg, de service aan de patiënt en gegevensbescherming en informatiebeveiliging op gespannen voet met elkaar staan. Bij het opstellen van beleid probeert het St. Antonius Ziekenhuis een zorgvuldige afweging te maken tussen deze belangen. Daarnaast blijft er ruimte voor medewerkers om gemotiveerd af te wijken mocht de situatie hiertoe aanleiding geven.

3.2. Beleidsdoelstellingen

Zoals uit bovenstaand blijkt, bevatten de onderwerpen privacy en gegevensbescherming en informatiebeveiliging grote mate van overlap. Tegelijkertijd zijn er ook verschillen. Privacy gaat over de gegevens van individuele personen. Informatiebeveiliging gaat over alle relevante organisatiegegevens, waar persoons- en patiëntengegevens onderdeel van uitmaken. Figuur 1 geeft dat weer. Deze paragraaf beschrijft de belangrijkste beleidsdoelstellingen voor beide onderwerpen.



FIGUUR 1: RELATIE TUSSEN GEGEVENSBESCHERMING EN INFORMATIEBEVEILIGING

De algemene doelstelling is de volgende:

> *Het aantoonbaar beheersen van de risico's op het gebied van gegevensbescherming en informatiebeveiliging zodat:*
> *(i) interne en externe belanghebbenden erop kunnen vertrouwen dat het St. Antonius Ziekenhuis zorgvuldig omgaat met informatie en*
> *(ii) het St. Antonius Ziekenhuis kansen kan benutten om zorg, onderwijs en onderzoek te verbeteren door de inzet van nieuwe informatiemiddelen.*

Hieronder valt onder meer:
- We voldoen aan toepasselijke wet- en regelgeving (compliant zijn), waaronder de AVG; het St. Antonius Ziekenhuis gaat conform vigerende wetgeving, op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen;
- Het St. Antonius Ziekenhuis is gecertificeerd voor NEN 7510 en ISO 27001;
- In aanvulling op de certificering informeren en rapporteren we aan onze interne en externe belanghebbenden (RvB, RvT) over de manier waarop we omgaan met gegevensbescherming en informatiebeveiliging;
- We onderhouden een control framework waarbij beheersmaatregelen aantoonbaar worden uitgevoerd.

3.3. Uitgangspunten beleid

Het proces van ‘gegevensbescherming en informatiebeveiliging’ begint met het definiëren van beleid. Het beleid biedt vervolgens een kader om (toekomstige) maatregelen in de gegevensbescherming en de informatiebeveiliging te toetsen aan vastgestelde best practices of normen en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen. Voor beide onderwerpen worden in deze paragraaf de beleidsuitgangspunten toegelicht.

3.3.1. Algemeen

De lijn is verantwoordelijk
Leidinggevenden dragen de primaire verantwoordelijkheid voor een zorgvuldige verwerking van informatie op hun afdeling/eenheid.

Leidinggevenden:
- informeren zichzelf over de risico's,
- sturen op risicobeheersing, en
- controleren of deze sturing effectief is.

Risicobeheersing omvat de keuze de uitvoering, handhaving van maatregelen en risicoacceptatie. Onder de lijnverantwoordelijkheid valt daarnaast de taak om het beleid met betrekking tot de verwerking van informatie te communiceren met alle relevante partijen, binnen de grenzen van het redelijke.
Een praktische vertaling van deze eis is dat het eigenaarschap van verbetermaatregelen standaard belegd is bij een lijnmanager (afdelingshoofd of manager) en niet bij een inhoudsdeskundige of een kwaliteitsfunctionaris. De lijnmanager legt hierover dus zelfstandig verantwoording af aan zijn eigen leidinggevende en/of de 2e en 3e lijns functionarissen.

Informatie is onder controle van het St. Antonius Ziekenhuis
Om informatiebeveiliging te borgen moet het St. Antonius ziekenhuis controle kunnen uitoefenen op de betreffende informatie. Deze moet daarom binnen de juridische, organisatorische en technische context van de organisatie worden bewaard, verwerkt en verstuurd. Het is om deze reden bijvoorbeeld niet toegestaan om gegevens op eigen laptops te plaatsen of deze met privé gebruikersaccounts van medewerker te uploaden naar Clouddiensten.

Geïnformeerde en risicogedreven besluitvorming
Bij wijzigingen, projecten en de aanschaf van informatiemiddelen is er een duidelijk beslismoment. Voorafgaand hieraan informeren lijn- en projectverantwoordelijken zich over de risico's, kansen, kosten en baten van een keuze m.b.t. gegevensbescherming en informatiebeveiliging en hoe deze zicht verhouden tot de bijdrage aan de strategische doelstellingen van de organisatie. Op basis van deze informatie nemen de verantwoordelijken een weloverwogen besluit en accepteren als nodig eventuele restrisico's. Zij borgen tevens de uitvoering van eventuele maatregelen.

Verantwoordelijkheden zijn ook in de keten geborgd
Het St. Antonius Ziekenhuis werkt nauw samen met ketenpartners waaronder andere ziekenhuizen maar ook bijvoorbeeld met leveranciers. Hierbij is er vaak sprake van complexe samenwerkingsverbanden, waaronder met maatschappen, in regionale overleggen en bij projecten. In deze situaties zijn verantwoordelijkheden voor het beheer en toegang tot een systeem of gegevens of het eigenaarschap van deze gegevens vaak gedeeld. Het is dan belangrijk dat alle partijen duidelijkheid hebben over hun taken en verantwoordelijkheden om te voorkomen dat deze niet uitgevoerd worden. Waar nodig zijn specifieke contractuele afspraken gemaakt en zijn informatiesystemen opgezet in overeenstemming met die bestaande contractuele afspraken. Samenwerkingsverbanden behoren daarnaast verantwoording af te leggen aan de betrokken organisaties en te kunnen aantonen dat afgesproken maatregelen ook daadwerkelijk zijn uitgevoerd.
Gegevensbescherming en informatiebeveiliging zijn ieders verantwoordelijkheid
Om de bovenstaande beleidsdoelstellingen te realiseren, wordt ook een beroep gedaan op onze medewerkers en onze organisatie. Van medewerkers, studenten, onderzoekers, PNIL, medisch specialisten en derden wordt verwacht dat ze zich integer gedragen en zorgvuldig omgaan met persoonsgegevens. Het is om deze reden dat er gedragsregels zijn geformuleerd en geïmplementeerd. Medewerkers worden gestimuleerd elkaar hierop aan te spreken.

Keten en cloud risico's
De organisatie is zich bewust van de risico's van missiekritische informatiesystemen (systemen waarvan de uitval een directe en/of zeer hoge impact kan hebben op het primaire proces). Een keuze om deze systemen buiten het St. Antonius Ziekenhuis te plaatsen bijvoorbeeld bij een externe (cloud) leverancier vereist daarom:
(i) een bestuursbesluit en
(ii) een gedocumenteerd en goedgekeurd business continuïteitsplan met ook aandacht voor de gevolgen van uitval in de regio.

Opleiding
Om ervoor te zorgen dat artsen en medewerkers voldoende kennis hebben en houden van de eisen voor rechtmatige verwerking van persoonsgegevens en informatiebeveiliging, is er structureel verplichte scholing op het gebied van gegevensbescherming en informatiebeveiliging. Dit gebeurt

tijdens elke introductiebijeenkomst voor nieuwe medewerkers en door middel van jaarlijkse e-learning modules. Ook geven inhoudsdeskundigen op verzoek of eigen initiatief specifieke voorlichting aan afdelingen.

3.3.2. Gegevensbescherming

Het St. Antonius Ziekenhuis onderschrijft de beginselen in de AVG[5] voor verwerking van persoonsgegevens. In dit hoofdstuk beschrijven we hoe we hieraan op hoofdlijnen invulling geven.

Rechtmatige, behoorlijke en transparante gegevensverwerking
Voor betrokkenen moet duidelijk zijn welke persoonsgegevens we verwerken, voor welke doelen we dat doen en hoe we deze gegevens verwerken. Die duidelijkheid bieden we in eerste instantie in onze privacyverklaring '*Privacyverklaring patiënten St. Antonius Ziekenhuis*' die we op onze website publiceren. Dit geldt onder andere voor gebruik van persoonsgegevens voor wetenschappelijk onderzoek en verwerkingen gebaseerd op de grondslag 'gerechtvaardigd belang'.
Voor medewerkers en sollicitanten is de *'Privacyverklaring medewerkers St. Antonius Ziekenhuis'* opgesteld.

Rechtmatige en behoorlijke verwerking betekent ook dat we steeds kritisch moeten nagaan of een bepaalde verwerking noodzakelijk is. Doordat het ziekenhuis een zeer grote hoeveelheid gegevens verwerkt, ontstaat de mogelijkheid om allerlei analyses uit te voeren of gegevens te verwerken voor aanvullende doeleinden (al dan niet in samenwerking met derden). Hoewel dit op zichzelf niet onmogelijk is, zal wel steeds een goede afweging moeten worden gemaakt of er een rechtmatige grondslag is om de verwerkingen uit te voeren.

Patiënten
De belangrijkste grondslag voor verwerking van patiëntgegevens is de behandelingsovereenkomst. Deze overeenkomst ontstaat automatisch zodra een patiënt medische zorg vraagt van het ziekenhuis. Voor de behandeling en financiële afwikkeling is het noodzakelijk om de patiëntgegevens te verwerken. Medewerkers en artsen die daarbij rechtstreeks betrokken zijn, mogen de gegevens verwerken. Voor de verwerking van de bijzondere categorieën persoonsgegevens (gegevens over gezondheid, seksueel gedrag of geaardheid en genetische gegevens) zijn de uitzonderingsregels van de AVG en Uitvoeringswet AVG (UAVG) van toepassing[6].

Ook worden patiëntgegevens verwerkt op grond van andere wetgeving. Dit geldt bijvoorbeeld voor kwaliteitsbewaking (denk ook aan registratie van incidenten of calamiteitenonderzoek[7] door adviseurs kwaliteit), declaraties aan zorgverzekeraars en verantwoording aan de IGJ. In de betreffende wetgeving is dan specifiek aangegeven dat bepaalde persoonsgegevens verwerkt mogen worden. Het is echter niet zo dat de algemene plicht voor het ziekenhuis om de kwaliteit te bewaken zondermeer een grondslag biedt voor allerlei verwerkingen. Dit zal steeds per verwerking goed moeten worden nagegaan. Een andere grondslag die daarbij betrokken kan worden, is 'gerechtvaardigd belang'.

De grondslag gerechtvaardigd belang wordt in het ziekenhuis soms gebruikt voor verwerkingen die van belang kunnen zijn voor de ontwikkeling van onze zorgverlening en bedrijfsvoering. Door (een deel van) de gegevens te gebruiken, kunnen we bijvoorbeeld de zorg efficiënter inrichten of kunnen we medische hulpmiddelen ontwikkelen. Indien wij de patiëntgegevens hiervoor willen gebruiken, maken we altijd een afweging tussen onze gerechtvaardigde belangen en het belang van de patiënt op gegevensbescherming (het te hanteren afwegingskader is in de bijlage A opgenomen). Ook selecteren we alleen die specifieke gegevens die noodzakelijk zijn voor het betreffende doel en zorgen we er (als uitgangspunt) voor dat de gegevens niet direct tot de patiënt te herleiden zijn (via pseudonimisering of anonimisering). Een overzicht van verwerkingen op deze grondslag en de afweging daarbij wordt door elke intern verantwoordelijke vastgelegd in het in het centrale

[5] Art. 5, lid 1 AVG
[6] Artikel 9, lid 1, sub h AVG en artikel 30, lid 3, sub a en lid 5 UAVG
[7] Bij calamiteitenonderzoek worden patiëntgegevens (grotendeels) gepseudonimiseerd door alleen initialen te gebruiken. Ook de IGJ ontvangt dus alleen initialen. Medewerkers worden alleen met de functietitel aangeduid en er is geen onderscheid meer tussen 'haar' en 'hem'. Elke medewerker wordt aangeduid met 'hem'. NB: op grond van het Uitvoeringsbesluit Wkkgz kan het noodzakelijk zijn nadere persoonsgegevens aan de IGJ te verstrekken (art. 8.1 t/m 8.6).

verwerkingsregister. Eenheden kunnen in meer detail hun eigen gegevensverwerkingen vastleggen mits deze gebaseerd zijn op specifiek gegevensbeschermingsbeleid en bekend zijn bij de FG.

Verder vinden verwerkingen plaats met toestemming van de patiënt. Dit is bijvoorbeeld het geval bij deelname aan bepaald wetenschappelijk onderzoek, patiëntenenquêtes, gebruik van het patiëntenportaal 'Mijn Antonius', voor uitwisseling van gegevens met andere zorgverleners (niet betrokken bij de behandelrelatie) of via een elektronisch uitwisselingssysteem. Bij wetenschappelijk onderzoek kan in heel specifieke situaties soms afgeweken worden van het uitgangspunt dat toestemming van de patiënt nodig is. Zie de toelichting in paragraaf 4.3.
De toestemming kan door patiënten te allen tijde net zo eenvoudig worden ingetrokken als dat deze gegeven is en heeft geen gevolgen voor de behandelrelatie.

Medewerkers
Voor verwerking van gegevens van medewerkers, stagiaires, A(N)IOS wordt de arbeids- en/of opleidingsovereenkomst als grondslag gebruikt. Voor personeel niet in loondienst (PNIL) betreft dat een 'overeenkomst gast' of 'overeenkomst externe'. Op basis van deze overeenkomst kunnen diverse verwerkingen plaatsvinden. Ook wetgeving biedt een grondslag voor verwerking, bijvoorbeeld voor fiscale verplichtingen of werkgever gerelateerde verplichtingen. Daarnaast kan gerechtvaardigd belang een grondslag bieden. Net als bij patiënten geldt dat er steeds een afweging moet worden gemaakt tussen de belangen van het ziekenhuis en die van de medewerker.
In werkgever-werknemer relaties kan een verwerking zeer zelden worden gebaseerd op toestemming. In het algemeen wordt ervan uit gegaan dat een werknemer te zeer afhankelijk is van de werkgever om echt vrije toestemming te kunnen geven. Het St. Antonius ziekenhuis baseert verwerkingen daarom meestal niet op toestemming. Dat geldt bijvoorbeeld wel voor het gebruik van foto's van medewerkers op de website. Indien een medewerker dit niet wil en dus geen toestemming geeft, wordt de foto niet gepubliceerd.

Sollicitanten
Voordat een medewerker wordt aangenomen, worden al persoonsgegevens verwerkt van sollicitanten. Deze verwerking kan nog niet worden gebaseerd op een arbeidsovereenkomst en wordt daarom gebaseerd op toestemming. Via de website gaan sollicitanten bij het insturen van de sollicitatie akkoord met de privacyverklaring die gelinkt is aan het digitale sollicitatieformulier.

Derden
Verwerking van persoonsgegevens van derden (bijv. patiëntvertegenwoordigers, gasten, contactpersonen van leveranciers en website bezoekers) baseren we op de betreffende overeenkomst, toestemming, gerechtvaardigd belang of een wettelijke verplichting.

Gegevensverwerkingen voldoen aan doelbinding
Persoonsgegevens mogen alleen verwerkt worden voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden'. Dit betekent dat per verwerking een specifieke doelomschrijving nodig is. Het is bijvoorbeeld onvoldoende om aan te geven dat de verwerking een betere bedrijfsvoering tot doel heeft of dat de verwerking bijdraagt aan de verbetering van de zorg. Deze omschrijvingen zijn te algemeen. Een betere omschrijving zou bijvoorbeeld kunnen zijn dat de verwerking noodzakelijk is om te onderzoeken of het gebruik van muziek bij een operatie onder narcose het herstel van een patiënt kan bespoedigen.
Een intern verantwoordelijke zal vóór aanvang van een nieuwe of aangepaste verwerking steeds het specifieke doel duidelijk moeten maken en daarbij ook de afweging moeten maken of dat een gerechtvaardigd doel is. Alle doeleinden worden uiteindelijk vastgelegd in het verwerkingsregister (zie ook paragraaf 5.4.1).

Patiënten
Van patiënten worden persoonsgegevens vooral verwerkt met als doel de behandeling van de patiënt en het verlenen van zorg. Dit betreft niet alleen identificerende gegevens, maar ook bijzondere persoonsgegevens (o.a. gezondheidsgegevens). De behandelaren, overige zorgverleners en anderen die direct bij de behandeling van de patiënt betrokkenen zijn (waaronder ook ondersteunend personeel) mogen deze gegevens verwerken (dit wordt onder meer gewaarborgd door een Break the Glass procedure in het EPD en door de goedgekeurde autorisatiematrix). Voorwaarde is dat zij gebonden zijn aan het beroepsgeheim of op andere wijze aan geheimhouding zijn gehouden. Alle artsen en medewerkers van het ziekenhuis voldoen aan deze eis, hetzij door hun beroepsgeheim, hetzij via de arbeids-, opleidings-, of opdrachtovereenkomst.

Andere belangrijke doelen van de verwerking van patiëntgegevens zijn (op hoofdlijnen) wetenschappelijk onderzoek, bewaking van de kwaliteit en veiligheid van zorgverlening binnen het ziekenhuis en bedrijfsmatige afwikkeling van de zorgverlening. Zoals hiervoor toegelicht zullen deze en overige verwerkingen nader moeten worden gespecificeerd. Voor wetenschappelijk onderzoek bestaat separaat beleid en voorlichtingsmateriaal.

Medewerkers en sollicitanten
De verwerking van persoonsgegevens van medewerkers heeft als belangrijkste doel een juiste verwerking van diverse arbeidsgerelateerde verplichtingen, zoals personeels- en salarisadministratie, verzuimadministratie en begeleiding, vergewisplicht (denk bijvoorbeeld aan BIG-registratie, VOG, diploma's, e.d.). Daarnaast worden gegevens verwerkt voor een zorgvuldig personeelsbeleid. Ook voor de Academie van het St. Antonius ziekenhuis is het noodzakelijk om persoonsgegevens te verwerken van medewerkers, stagiaires en A(N)IOS ten behoeve van opleiding en ontwikkeling. Voor de selectie en aanname van nieuwe personeelsleden worden gegevens van sollicitanten verwerkt.

Derden
Verwerking van persoonsgegevens van derden is noodzakelijk ten behoeve van goede en veilige zorg aan patiënten (zoals gegevens van patiëntvertegenwoordigers), ter bescherming van medewerkers en patiënten (denk aan gele en rode kaarten en cameratoezicht), voor bezoek aan onze website of andere nader omschreven doeleinden (bijvoorbeeld klachtafhandeling door een nabestaande).

Minimale gegevensverwerking (dataminimalisatie), juistheid van gegevens en opslagbeperking
Het beginsel van dataminimalisatie in de AVG dwingt verantwoordelijken om alleen die persoonsgegevens te verwerken die noodzakelijk en toereikend zijn om het beoogde doel te realiseren[8].
Voor een betrokkene gaat het daarbij om drie aspecten:
- Welke gegevens worden verzameld;
- In welke systemen staan deze gegevens;
- Hoelang worden deze gegevens bewaard.

Indien het doel op een andere manier of met minder persoonsgegevens kan worden gerealiseerd, dan zal de verwerking (van een deel van de persoonsgegevens) achterwege moeten blijven of zodanig moeten worden aangepast dat alleen de minimaal noodzakelijk gegevens worden verwerkt. Intern lijnverantwoordelijken zullen daarom steeds de afweging moeten maken en in het verwerkingsregister moeten vastleggen welke persoonsgegevens strikt noodzakelijk zijn om het door hen bepaalde doel te realiseren.

Bewaartermijnen
Dataminimalisatie vereist ook dat de opslag van de gegevens beperkt wordt tot een strikt minimum. Indien mogelijk moeten persoonsgegevens na realisatie van het doel vernietigd worden, tenzij er gerechtvaardigde redenen zijn om de gegevens langer te bewaren. In relatie tot de behandeling van de patiënt is de WGBO (Wet geneeskundige behandelingsovereenkomst) hierin leidend. Het St. Antonius Ziekenhuis gebruikt zo veel mogelijk technische maatregelen voor vernietiging maar kan ook organisatorische maatregelen toepassen.

[8] Ook wel de toetsing aan de beginselen van subsidiariteit en proportionaliteit

De opslagtermijn van gegevens van medewerkers is vooral bepaald door wetgeving, o.a. door de administratieplicht van 7 jaar.
Voor alle verwerkingen hebben intern verantwoordelijken bewaartermijnen bepaald, hetzij op grond van wetgeving, hetzij op grond van het ziekenhuisbeleid. In het dataretentiebeleid zijn de algemene bewaartermijnen vastgelegd.

Vertrouwelijkheid en integriteit
Het spreekt voor zich dat de persoonsgegevens juist en actueel moeten zijn om goede zorg aan onze patiënten te kunnen verlenen en om onze verplichtingen als werkgever/opdrachtgever na te kunnen komen. Ook moet de vertrouwelijkheid van gegevens te worden gewaarborgd, bijvoorbeeld om datalekken te voorkomen. Hierdoor worden er strikte eisen gesteld aan de beveiliging van de persoonsgegevens.

Bij de inschrijving van patiënten of aanname van personeel wordt de identiteit van de betrokkene gecontroleerd en worden desbetreffende gegevens vastgelegd. In het medisch dossier worden gegevens verwerkt door behandelaren en andere zorgverleners. Zij nemen die gegevens op die noodzakelijk zijn voor de goede zorg of die anderszins van belang zijn voor de behandeling van de patiënt. Ook de patiënt zelf kan een deel van zijn medisch dossier rechtstreeks inzien (via ‘Mijn Antonius’) en de juistheid van de gegevens controleren.

Persoonsgegevens worden zoveel mogelijk in één bronbestand verwerkt zodat de juistheid het best kan worden gewaarborgd. Dit betekent dat medewerkers niet zelf nog extra bestanden aanleggen waarin delen van persoonsgegevens worden opgeslagen om dat vervolgens weer als bron te gebruiken. Het ziekenhuis gebruikt bijvoorbeeld het EPD als centraal systeem voor patiëntgegevens ten behoeve van de behandelingsovereenkomst. Daarnaast worden aanvullend systemen en software gebruikt voor specifieke verwerkingen. Dit betreft bijvoorbeeld röntgenbeelden, hartfilmpjes, labanalyses, etc. De verschillende systemen worden wel zoveel mogelijk aan elkaar gekoppeld om de juistheid van de gegevens te waarborgen.
Door de afdeling BI worden dagelijks op basis van zorgvuldige selectie (in het kader van dataminimalisatie) gegevens “As-Is” uit de systemen verzameld en opgeslagen in een database (op het BI platform) ten behoeve van verdere verwerkingen. Het BI platform wordt derhalve gezien als doorkijksysteem naar de verschillende bronnen. Voor medische beslissingen blijft het EPD de enige bron, al dan niet ondersteund met grafische weergave van geaggregeerde gegevens uit het BI platform. Voor verwerkingen van patiëntgegevens (voor andere doelen dan de behandeling) wordt zoveel mogelijk gebruik gemaakt van het BI platform. Alleen als het echt niet anders kan, worden persoonsgegevens ook in andere bestanden opgenomen, maar dienen deze niet als bron voor andere verwerkingen.

Delen met derden
In het geval van samenwerking met externe partijen, waarbij er sprake is van gegevensverwerking van persoonsgegevens, maakt het St. Antonius Ziekenhuis afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. Het St. Antonius Ziekenhuis houdt voor zover dat mogelijk is vanuit de eigen positie toezicht op de naleving van deze afspraken.

Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokkene (o.a. patiënt en medewerker) zoveel mogelijk beperkt.

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Rechten van betrokkenen
Natuurlijke personen waarvan het St. Antonius Ziekenhuis de persoonsgegevens verwerkt, hebben het recht op inzage, correctie, inperking gebruik, verwijdering en dataportabiliteit. Dataportabiliteit geeft patiënten de mogelijkheid om hun gegevens makkelijk door te geven aan een ander ziekenhuis. Het intrekken van toestemming voor verwerking zal op vergelijkbare wijze als het geven van toestemming worden ondersteund. Op de website van St. Antonius Ziekenhuis kan de betrokkene de werkwijze inzien.

Het St. Antonius Ziekenhuis vindt het vanzelfsprekend om zorgvuldig, vertrouwelijk en betrouwbaar om te gaan met persoonsgegevens van patiënten, medewerkers en andere betrokkenen. Daarbij hoort ook dat de organisatie kan aantonen hoe dat gebeurt en dat betrokkenen eenvoudig hun rechten kunnen uitoefenen. Goede informatievoorziening is daarvoor essentieel. In de privacyverklaringen licht de organisatie zo bondig mogelijk, maar wel volledig toe hoe aan de eisen van de AVG is voldaan en welke rechten betrokkenen kunnen oefenen. Binnen het ziekenhuis zijn de processen zodanig ingericht dat de afhandeling van die rechten van betrokkenen daadwerkelijk eenvoudig realiseerbaar is. Hieronder volgt een beknopt overzicht van de rechten van betrokkenen en hoe we deze in de organisatie hebben geborgd.

Intrekking toestemming
Als een verwerking is gebaseerd op toestemming van de betrokkene, dan moet de betrokkene de toestemming op elk moment kunnen intrekken. Het intrekken van toestemming moet net zo eenvoudig zijn als het geven van toestemming. Bij (wetenschappelijk) onderzoek met gegevens is het intrekken van toestemming mogelijk door een procedure die is vastgelegd in het toestemmingsformulier. Ook bij andere verwerkingen dienen interne verantwoordelijken ervoor te zorgen dat een procedure voor het intrekken van toestemming is geborgd.

Recht op inzage en afschrift
Een betrokkene heeft recht op inzage in of een kopie van de gegevens die het St. Antonius Ziekenhuis verwerkt. Patiënten kunnen de gegevens die in het kader van de behandelingsovereenkomst worden verwerkt inzien via Mijn Antonius. Ze krijgen daarmee inzicht in een deel van hun medisch dossier. Een andere optie is dat zij een kopie of inzage vragen bij de behandelend arts of via het Servicepunt (deze werkwijze geldt ook voor medewerkers die tevens patiënt zijn in ons ziekenhuis). Inzage in overige verwerkingen die geen onderdeel uitmaken van het medisch dossier, kunnen patiënten opvragen bij het Servicepunt.
Medewerkers hebben soms zelf inzage in de gegevens die verwerkt zijn (bijvoorbeeld via hun personeelsdossier) of kunnen inzage of een kopie vragen via hun leidinggevende.

Recht op correctie
Als feitelijke persoonsgegevens onjuist zijn geregistreerd (bijv. een naam is verkeerd gespeld of een geboortedatum klopt niet), dan kan een betrokkene deze gegevens laten aanpassen bij de centrale inschrijfbalie of via Mijn Antonius. Medewerkers kunnen dit zelf regelen via het Mijn portaal van HR of via hun leidinggevende, respectievelijk de HR Servicedesk.
NB: voor correcties in het medische dossier gelden ook andere regels op grond van de WGBO. Verzoeken tot wijziging van gegevens in het medisch dossier, dienen altijd met de zorgverlener(s) te worden afgestemd.

Recht om vergeten te worden of gegevens uit het medisch dossier te laten vernietigen
Een betrokkene kan een verzoek indienen bij het Service Punt om (een deel van) de verwerkte persoonsgegevens te vernietigen. Het St. Antonius Ziekenhuis is verplicht hieraan gehoor te geven, tenzij dit strijdig is met de doelen waarvoor de gegevens verwerkt worden of als dit strijdig is met andere wetgeving. Een verzoek tot vernietiging van (een deel van) het medisch dossier moet altijd met de zorgverlener(s) te worden afgestemd.

Recht op beperking van de verwerking
In plaats van vernietiging van gegevens kan een betrokkene ook verzoeken om een (tijdelijke) beperking van de verwerking. Bijvoorbeeld gedurende de periode waarin het St. Antonius Ziekenhuis een verzoek tot correctie van gegevens of een bezwaar tegen verwerking van gegevens behandelt.

Recht op dataportabiliteit (gegevensoverdraagbaarheid)
Dit recht houdt in dat een betrokkene persoonsgegevens, die volledig via een automatisch proces worden verwerkt (bijv. het digitaal toezenden van gegevens via Mijn Antonius), kunnen laten overdragen aan een andere (zorg)aanbieder. Dit geldt alleen als deze automatische verwerking is gebaseerd op toestemming van de betrokkene of op grond van een overeenkomst.

Recht om bezwaar te maken
Indien het St. Antonius Ziekenhuis persoonsgegevens verwerkt op basis van een voor ons gerechtvaardigd belang, dan moet een betrokkene altijd bezwaar kunnen maken tegen deze verwerking en moet het St. Antonius Ziekenhuis de verwerking te beëindigen indien de hernieuwde belangenafweging ten gunste van de betrokkene uitvalt. Zie ook de informatie over deze grondslag in paragraaf 3.1 “Grondslagen voor de verwerkingen”.

Bovenstaande verzoeken van patiënten, kunnen worden ingediend bij het Servicepunt. Medewerkers kunnen een verzoek indienen bij hun leidinggevende. Na ontvangst van een verzoek om een of meer van deze rechten uit te oefenen, informeert het St. Antonius Ziekenhuis de betrokkene binnen een maand hoe hieraan voldaan zal worden. Indien mogelijk wordt het verzoek binnen een maand afgehandeld.

Klachtrecht
Betrokkenen kunnen voor klachten over de verwerking van hun persoonsgegevens contact opnemen met de FG. Mocht dit niet naar tevredenheid van betrokkenen worden afgehandeld, of als een betrokkene dat wil, kan een klacht ook rechtstreeks worden ingediend bij de AP.

Gegevensbeschermingseffectbeoordeling
Met een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment; DPIA) worden de effecten en risico’s van nieuwe of bestaande diensten/verwerkingen beoordeeld op de bescherming van de privacy. Het St. Antonius Ziekenhuis voert deze uit indien:
- Op grote schaal bijzondere persoonsgegevens worden verwerkt (o.a. medische gegevens);
- Op grote schaal en systematisch mensen worden gemonitord in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

De eigenaar van de dienst/service/systeem is verantwoordelijk voor de uitvoering van de DPIA en kan de PO, CISO en FG hierbij betrekken. De werkwijze van de DPIA is beschikbaar in het St. Antonius Ziekenhuis, inclusief een format rapportage.

Inzet van camera’s
Binnen het ziekenhuis wordt gebruik gemaakt van cameratoezicht. Cameratoezicht wordt in sommige gevallen gebruikt voor de behandeling van patiënten maar ook voor andere doeleinden, waaronder het vergroten van de veiligheid in de openbare ruimten binnen het ziekenhuis. Camera’s kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen plaatsen we alleen camera’s wanneer er geen andere manieren zijn om het doel te bereiken. Bezoekers en medewerkers attenderen we op het gebruik van camera’s. Door toevoegingen van camera’s of verandering van locaties wordt het camerabeleid van het St. Antonius Ziekenhuis constant geactualiseerd.

Incidenten
Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen het St. Antonius Ziekenhuis noemen we een privacy-incident. De bekendste vorm van een dergelijk incident is een datalek. Medewerkers zijn verplicht om een (vermoedelijk) ‘datalek’ en andere privacy-incidenten direct te melden via het meldformulier datalekken. Indien de melder daar de voorkeur aan geeft kan dit ook vertrouwelijk bij de FG. ICT incidenten moeten worden gemeld aan de I&I service desk.
Van elk incident en de afhandeling daarvan wordt een registratie bijgehouden. (Datalek) Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen

persoonlijke consequenties heeft. Een melder moet zolang het incident nog niet is afgehandeld vertrouwelijk met de melding om te gaan en hierover niet te communiceren met betrokkenen of anderen. De afhandeling van incidenten heeft als doel het probleem op te lossen, de schade te beperken en de wetgeving na te leven. Niet elk incident leidt tot een datalek.

Datalekken
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben of wanneer gegevens verloren zijn gegaan. Wanneer er een datalek heeft plaatsgevonden meldt het St. Antonius Ziekenhuis dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan het AP. De FG brengt het verantwoordelijk lid van de RvB hiervan op de hoogte. Als de melding later is dan 72 uur, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt het St. Antonius Ziekenhuis dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Ondanks alle maatregelen kan het toch gebeuren dat er een incident plaatsvindt met betrekking tot persoonsgegevens. Dit wordt een datalek genoemd. Een datalek kan op veel verschillende manieren plaatsvinden, bijvoorbeeld door een recept mee te geven met de verkeerde patiënt, gegevens door te sturen naar een verkeerde organisatie, zonder toestemming van betrokkene gegevens te delen, een hack in ons ICT-systeem of installatie van malware, etc. Ook als persoonsgegevens onbedoeld verloren gaan, spreken we van een datalek. Elke medewerker die een datalek ontdekt, moet deze direct (binnen 24 uur) te melden door middel van een digitaal formulier (zie hoofdstuk 5.2). De FG wordt hierdoor automatisch geïnformeerd zodat vervolgstappen snel kunnen worden opgepakt. Dit betreft in ieder geval beoordeling of het datalek aan de AP en betrokkenen moet worden gemeld en of maatregelen moeten worden getroffen om het datalek te verhelpen.

Een bijzondere situatie doet zich voor indien er bij een andere organisatie sprake is van een datalek met gegevens van onze patiënten of medewerkers. Denk bijvoorbeeld aan een incident bij de verwerker van salarisgegevens of een incident bij een samenwerkingspartner zoals Santeon. In die gevallen is het ziekenhuis nog steeds (mede)verantwoordelijk voor de melding en afhandeling van het datalek, maar zijn we ook afhankelijk van deze organisaties om het datalek te melden. Daarvoor maken we specifiek afspraken met deze organisaties. Voor verwerkers doen we dit bij voorkeur met het model verwerkersovereenkomst van de BOZ. Voor andere partners leggen we dit vast in een samenwerkingsovereenkomst.

Alle datalekken worden geregistreerd en ook de Raad van Bestuur wordt over de datalekken geïnformeerd. Om datalekken te voorkomen, kunnen we op basis van veel voorkomende soorten datalekken ons beleid specifiek aanscherpen of onze voorlichting en scholing aan medewerkers verbeteren.

Privacy by default en by design
Bij het werken volgens Privacy by Design wordt bij de start van het ontwerp van een dienst of informatiesysteem rekening gehouden met privacy. De aandacht voor privacy blijft tijdens de gehele levensduur van het systeem bestaan. Het doel is de beveiliging van persoonsgegevens te optimaliseren. Ook moet rekening worden gehouden met de hele levenscyclus van de data: opslag, mutaties en verwijdering. Naast de technische aspecten spelen ook organisatorische aspecten een rol. Privacy by Design wordt vaak in één adem genoemd met Privacy by Default. Het zijn verwante begrippen; Privacy by Default betreft de standaard instellingen van een programma, website, dienst of apparaat.

Gegevensuitwisseling met derden
Voor de gegevensuitwisseling met derden en t.b.v. medisch wetenschappelijk onderzoek zijn specifieke afspraken met de afdeling Research & Development (R&D) gemaakt en vastgelegd in het beleid gegevensuitwisseling voor kwaliteitsregistraties en wetenschappelijk onderzoek. Dit geldt ook voor het uitwisselen van persoonsgegevens met partijen buiten het St. Antonius Ziekenhuis ten behoeve van regionale en landelijke kwaliteitsregistraties. Voor het uitwisselen van medische gegevens onderschrijft het St. Antonius Ziekenhuis de noodzaak voor standaardisatie en streeft hierbij

ook technische ICT-standaarden in de zorg na (Nictiz, IHE). Het handhaven van beveiliging van informatie (en programmatuur) die wordt uitgewisseld binnen een organisatie en vooral met externe entiteiten maakt deel uit van de NEN 7510. Per categorie gegevens en per categorie externe partij wordt vastgesteld of uitwisseling van gegevens is toegestaan en onder welke voorwaarden en met welke maatregelen. Deze regels gelden voor alle persoonsgegevens van patiënten en van medewerkers.

3.3.3. Informatiebeveiliging

Kwetsbaarheden moeten worden verholpen
De aard van ICT risico's is dat er altijd een kans bestaat op een gebeurtenis met een enorme impact die zich nog nooit heeft voorgedaan en zelfs niet voorstelbaar was. (Een zogenaamde "black swan"). Wie risico's baseert op historisch verloop en terugkijkt naar de vorige incidenten en gebeurtenissen schat om deze reden de risico's waarschijnlijk te laag in. Dit realiserende moeten kwetsbaarheden in ICT systemen zoveel mogelijk worden verholpen ongeacht de ernst ervan.

Aantoonbaar in control
Het risico bestaat dat informatiebeveiliging een papieren tijger wordt. Om dit risico te beperken streeft de organisatie aantoonbare implementatie na. Hierbij leveren afdelingen informatie aan die aantoont dat ze de processen hebben uitgevoerd volgens geldende afspraken.

De eenheid I&I wordt altijd betrokken bij aanschaf en beheer van ICT diensten
De CISO, PO en FG werken samen met de eenheid I&I om de informatievoorziening op een efficiënte manier te beveiligen. Organisatieonderdelen mogen niet buiten deze governance om werken.

4. Vertaling naar onze organisatie

4.1. Wijze van uitvoering van beleid

Het is nadrukkelijk de bedoeling dat informatiebeveiliging een integraal onderdeel uitmaakt van de totale bedrijfsvoering in onze organisatie en op elk niveau. Op basis van het Information Security Management Systeem (ISMS) wordt informatiebeveiliging als een continu proces conform de Deming circle (plan-do-study-act) vormgegeven in onze organisatie.

Opstelling, bijstelling en goedkeuring
Dit beleidsdocument wordt jaarlijks bijgesteld, of zoveel vaker, om de effectiviteit te waarborgen. De RvB stelt het beleid formeel vast, na review en advies door de bestuursadviescommissie gegevensbescherming en informatiebeveiliging.

Waar nodig stelt de organisatie aanvullende kwaliteitsdocumenten (beleid, gedragscodes, procedures en protocollen) op om concrete invulling te geven aan het hoofdbeleid.

Indien het aanmaken, wijzigen of terugtrekken van beleid aanzienlijke impact heeft op de werkwijze van de organisatie vindt consultatie hierover plaats met de leidinggevenden van de betreffende medewerkers, de bestuursadviescommissie gegevensbescherming en informatiebeveiliging en/of de adviesgremia zowel intern (OR) als extern (cliëntenraad).
Organisatieonderdelen zijn daarnaast bevoegd om hun eigen kwaliteitsdocumenten op te stellen, mits deze:

- Niet strijdig zijn met het bestaande beleid of het vervangen[9];
- Onderworpen zijn aan een eigen jaarlijkse updatecyclus;
- Gecommuniceerd worden naar de CISO, PO en FG.

De Corporate Information Security Officer (CISO) en de Privacy Officer (PO) van het St. Antonius Ziekenhuis zijn verantwoordelijk voor het beleid omtrent gegevensbescherming en onderhouden dit document periodiek. Hun rollen worden in hoofdstuk 5 nader toegelicht.

4.2. Meten van voortgang en bijsturing

De organisatie onderhoudt een control framework om aantoonbaar bewijs te verzamelen van de uitvoering van NEN 7510 en ISO 27001 beheermaatregelen en waar nodig bij te sturen bij geconstateerde afwijkingen (gebreken in opzet, bestaan en werking). Het programma is opgezet aan de hand van procedures of vragenlijsten die met een vooraf gedefinieerde frequentie (dag, week, maand, kwartaal, jaar, bij optreden) worden uitgevoerd onder verantwoordelijkheid van een eigenaar. Acties voortkomend uit het control framework programma worden in de centrale gegevensbescherming en informatiebeveiliging actielijst bijgehouden.
Het control framework programma integreert met het tracer audit programma van de afdeling Kwaliteit & Patiëntveiligheid (K&PV): De kwaliteitsauditors (aangesteld door K&PV) voeren vastgestelde procedures / vragenlijsten uit tijdens de tracer audits. De PO en CISO lopen mee met de audits als inhoudsdeskundigen. De PO en CISO en de afdeling K&PV overleggen voorafgaand aan de tracer audits over toepassingsgebied, de specifieke vragenlijsten, de inzet van mensen en middelen en planning.
Driemaandelijks brengen de PO en CISO verslag uit van de uitvoering van het control framework bij de bestuursadviescommissie gegevensbescherming en informatiebeveiliging. De bestuursadviescommissie gegevensbescherming en informatiebeveiliging ontvangt per kwartaal een compleet overzicht. Deze rapportage wordt daarna via de afdeling ARC gebundeld met andere rapportages en voorgelegd aan de RvB. Op basis van deze rapportage kan de RvB een inschatting maken van de risico's die we op dat moment lopen ten aanzien van vigerende wet- en regelgeving en een inschatting maken in welke mate, in welk tempo of in welke volgorde we aan onze beleidsdoelen willen voldoen.

[9] Indien een organisatieonderdeel materieel afwijkt van het hoofdbeleid moet een risicoanalyse plaats vinden. De PO/CISO legt deze uitzondering vast in het centrale risicoregister.

4.3. Hoe communiceren we hierover naar collega's

Het St. Antonius Ziekenhuis vindt de bescherming van de persoonlijke levenssfeer van patiënten en van medewerkers van groot belang. In afstemming met Marketing & Communicatie wordt door de PO en CISO een 'Communicatieplan' uitgevoerd. In dit communicatieplan staat beschreven welke activiteiten worden uitgevoerd om het belang van gegevensbescherming en informatiebeveiliging zo efficiënt en effectief mogelijk onder de aandacht te brengen bij onze medewerkers. Onderdeel van het Communicatieplan is in elk geval:

- Nieuwe medewerkers worden op hun eerste werkdag geïnformeerd over dit beleid, het St. Antonius Ziekenhuis vraagt medewerkers hier kennis van te nemen en bij te dragen aan het uitvoeren van het beleid;
- Alle nieuwe medewerkers krijgen een verplichte security awareness training van circa 30 minuten over hun algemene verantwoordelijkheden;
- Specifieke doelgroepen krijgen face-to-face trainingssessies of ander voorlichtingsmateriaal (bijvoorbeeld de informatiemanagers en leidinggevenden);
- Alle beleidsdocumenten zijn beschikbaar op Kwaliteitsnet;
- De RvB communiceert (bijvoorbeeld middels een email of blog) jaarlijks over het belang van informatiebeveiliging naar de medewerkers.

Omdat het St. Antonius Ziekenhuis NEN 7510 én ISO 27001 gecertificeerd is kunnen niet alleen alle toezichthouders, maar ook onze collega zorgverleners, zorgverzekeraars en vooral onze patiënten zelf vaststellen dat we voldoen aan algemeen geaccepteerde vereisten en dat patiëntgegevens bij ons in goede handen zijn.[10]

4.4. Incident management procedure

Een informatiebeveiligingsincident is een afzonderlijke gebeurtenis of een reeks informatiebeveiligingsgebeurtenissen waarvan het zeer waarschijnlijk is dat deze de bedrijfsactiviteiten compromitteren en de informatiebeveiliging in gevaar brengen.

Geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging moeten worden gemeld. Ieder organisatieonderdeel is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. Dergelijke signalen en meldingen zijn randvoorwaardelijk om de schade te beperken en de continuïteit van de bedrijfsvoering te borgen. De evaluatie van beveiligingsincidenten wordt eveneens benut voor het continu verbeteren van informatiebeveiliging.

Voor het beheer en de registratie van informatiebeveiligingsincidenten is een meldpunt ingericht. Het melden van dergelijke incidenten moet gedaan worden bij de I&I Helpdesk waar de incidenten in het ticketsysteem geregistreerd en geclassificeerd en geprioriteerd worden voor een correcte afhandeling. Voor het melden van datalekken is een separate meldingsprocedure door de FG gemaakt. Tabel 1 geeft aan hoe verschillende soorten incidenten gemeld kunnen worden.

TABEL 1: MELDEN VAN VERSCHILLENDE SOORTEN INCIDENTEN

Type incident	Werkwijze
Datalekken	Vanaf werkplek Start > Datalek melden
Informatiebeveiligingsincidenten	Tijdens kantoortijden per email aan de I&I Service desk Buiten kantoortijden per telefoon aan de I&I Service desk (alleen bij grote incidenten)
Zorggerelateerde incidenten	Veilig Incident Melden / Melden incident medewerker: Vanaf werkplek: Start > Incidentmelding VIM en MIM

[10] Certificaten zijn beschikbaar via de publieke website op https://www.antoniusziekenhuis.nl/privacy-en-veiligheid.

5. Governance

5.1. Besturing van de organisatie

De Raad van Bestuur is eindverantwoordelijk voor alle gegevensverwerkingen van het St. Antonius Ziekenhuis. De verantwoordelijkheden worden in de lijn belegd, waarbij iedere medewerker in overeenstemming met zijn rol een eigen verantwoordelijkheid heeft. De Privacy Officer (PO) en de Corporate Information Security Officer (CISO) opereren vanuit de tweede lijn voor respectievelijk gegevensbescherming en informatiebeveiliging. De Functionaris gegevensbescherming (FG) opereert vanuit de derde lijn. FG en CISO zorgen voor updates van het beleid en het verbeterprogramma gegevensbescherming en informatiebeveiliging. Hun rol en verantwoordelijkheid wordt onderstaand nader toegelicht[11].

Functionaris Gegevensbescherming (FG)
De FG ziet toe op de implementatie van de Algemene Verordening Gegevensbescherming inclusief de gegevensuitwisseling met derden. De FG toetst periodiek en onafhankelijk of adequate maatregelen zijn getroffen om risico's te beheersen, in samenwerking met Internal Audit.

Privacy Officer (PO)
De PO is met name actief op strategisch niveau en stelt samen met de CISO het gegevensbescherming en informatiebeveiligingsbeleid en privacyverklaring op en adviseert de organisatie en personen over privacyvraagstukken.

Corporate Information Security Officer (CISO)
De CISO heeft hierbij met name een rol op strategisch niveau. Zijn taak is te waken over informatiebeveiliging.

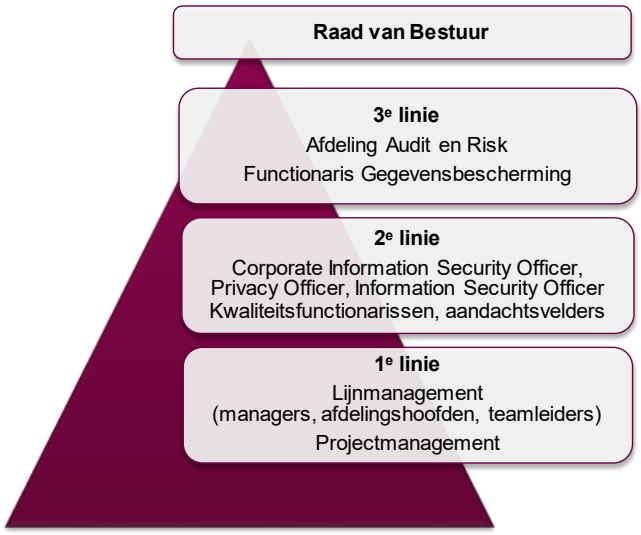
ISOs en kwaliteitsfunctionarissen
Op tactisch niveau stellen ISOs en andere kwaliteitsfunctionarissen beleid op en waken over het uitvoeren van verbetermaatregelen.

Aandachtsvelders
Op operationeel niveau kan per eenheid een ISO en/of aandachtsvelder vrijgemaakt worden om enkele uren per week specifiek te werken aan instandhouding en verbetering van gegevensbescherming en informatiebeveiliging, bijvoorbeeld voor het beantwoorden van vragen, het wijzen op (mogelijke) datalekken, het uitvoeren van tracer audits en om bewustwording te creëren voor het zorgvuldig om te gaan met gegevens van patiënten en medewerkers.

Three Lines model
Het St. Antonius Ziekenhuis heeft gekozen voor het "Three Lines model". Dit model (weergegeven in Figuur 2) is het uitgangspunt voor het sturen op gegevensbescherming en informatiebeveiliging.

1. De eerste lijn bestaat uit het lijn- en projectmanagement en is verantwoordelijk voor het uitvoeren van het beleid voor de eigen afdeling, team of project. De eerste lijn toont aan met rapportages dat zij beheersmaatregelen waarvoor zij verantwoordelijk is daadwerkelijk uitvoert en waar nodig bijstuurt en consulteert waar nodig de tweede lijn. De eerste lijn accepteert risico's en geeft goedkeuring aan de uitvoering van projecten.
2. De tweede lijn stelt het beleid op, voert algemene risico assessments uit en ondersteunt, adviseert en bewaakt de uitvoering van de eerste lijn. De PO, CISO en de ISO coördineren de activiteiten voor respectievelijk gegevensbescherming en informatiebeveiliging, geholpen door kwaliteitsfunctionarissen en aandachtsvelders.
3. De derde lijn houdt toezicht op de activiteiten van de eerste en tweede lijn. De derde lijn bestaat uit de afdeling Internal Audit en de FG. De afdeling Internal Audit voert interne audits uit en rapporteert direct aan het bestuur. De FG houdt voor de Autoriteit Persoonsgegevens toezicht op de uitvoering van de AVG en rapporteert eveneens direct aan het bestuur.

[11] De overige, aanpalende rollen die verantwoordelijkheid hebben in het realiseren van het in dit beleid genoemde doelstellingen zijn opgenomen in sectie 5.3.



FIGUUR 2: DE THREE LINES VOOR GEGEVENSBESCHERMING EN INFORMATIEBEVEILIGING

Geven van managementadvies
In voorkomende gevallen geven CISO, PO en FG en andere functionarissen advies aan het management over gegevensbescherming en informatiebeveiliging. Hierbij gaat het om drie soorten adviezen:

1. Adviezen over het verbeteren van gegevensbescherming en informatiebeveiliging. Hierbij zijn er geen concrete risico's te beheersen maar zijn er kansen om gegevensbescherming en informatiebeveiliging te versterken.
2. Adviezen over concrete probleempunten waarvan de inschatting is dat de risico's binnen de risicobereidheid van de organisatie vallen.
3. Adviezen over risico's die duidelijk boven de risicobereidheid van de organisatie vallen. Dit behoort in het advies duidelijk beschreven te zijn.

Overeenkomstig het staande risicomanagement beleid voor gegevensbescherming en informatiebeveiliging en de behandeling van risico's is het management niet verplicht om adviezen van type één en twee op te volgen. Voor het derde type advies is een expliciete risicoacceptatie of behandelplan wel noodzakelijk.

5.2. Overlegstructuren

Bestuursadviescommissie Gegevensbescherming & Informatiebeveiliging
Deze adviescommissie is aangesteld door de RvB en heeft een adviserende rol naar de CFO van de Raad van Bestuur ten aanzien van het gegevensbescherming en informatiebeveiliging:

- De commissie is een adviesorgaan naar de CFO binnen de Raad van Bestuur ten aanzien van besluiten met betrekking tot gegevensbeschermings- en informatiebeveiligingsbeleid.
- De commissie monitort de voortgang van de genomen besluiten.
- De commissie brengt, op verzoek dan wel op eigen initiatief, advies uit aan de Raad van Bestuur over:
  - Aangelegenheden die in relatie staan tot gegevensbescherming van patiënten, medewerkers en hun onderlinge relatie en die in relatie staan met de stichting;
  - Aangelegenheden die in relatie staan tot informatiebeveiliging van de stichting;
  - Het goedkeuren van relevante beleidsdocumenten;
  - In voorkomende gevallen bereidt de bestuursadviescommissie (voorgenomen) RvB-besluiten inhoudelijk voor of geeft hier advies over.
- De commissie stelt beleidsdocumenten vast, die niet de noodzakelijke goedkeuring van de Raad van Bestuur behoeven.[12]

[12] Dit betreft kleine wijzigingen, onderhoudsversies en nieuwe beleidsdocumenten met beperkte impact (ter beoordeling aan de bestuursadviescommissie gegevensbescherming en informatiebeveiliging).

- De commissieleden zorgen voor terugkoppeling naar de achterban van besluiten en brengen agendapunten vanuit de achterban in via de secretaris van de commissie.
- De commissie heeft geen normstellende bevoegdheden bij het bepalen van de inrichting van het elektronische patiëntendossier.
- De commissie rapporteert tenminste twee per jaar aan de RvB CFO.
- De commissie vergadert elke maand volgens een door de Raad van Bestuur vastgesteld reglement.

De gegevensbescherming en informatiebeveiliging gerelateerde adviezen worden door respectievelijk de FG en de CISO tijdens het periodieke overleg met de portefeuillehouder van de Raad van Bestuur toegelicht en besproken. Terugkoppeling vindt altijd aan de commissie plaats. Vanuit hun functie hebben de CISO, PO en FG een eigen adviesrecht zoals vastgelegd in het reglement.

Rapportage
CISO rapporteert elk kwartaal aan de commissie. In deze rapportage zijn opgenomen:
- Adviezen
- Status van risicobeheersing
- Ontwikkelingen in de omgeving (wet- en regelgeving, klanten, leveranciers, samenwerkingsverbanden, dreigingen[13])
- Wijzigingen in beleid
- Status van uitvoering inclusief datalekken en andere incidenten
- Interne audits en controles
- Verbetermaatregelen

Gegevensbescherming en informatiebeveiliging overleg
De CISO, PO, en FG en assistent FG overleggen tweewekelijks. Deze vergadering dient als voorbereiding voor de bestuursadviescommissie.

Directiebeoordeling
Jaarlijks vindt een directiebeoordeling door de RvB plaats conform NEN 7510 en ISO 27001.
Dit is inclusief:
- Het vaststellen van het beleid gegevensbescherming en informatiebeveiliging en de informatiebeveiligingsdoelstellingen, zodat deze (blijven) aansluiten bij de strategische richting van de organisatie;
- Het evalueren of het managementsysteem voor gegevensbescherming en informatiebeveiliging zijn beoogde resultaten behaalt;
- De beoordeling welke verbeteringen doorgevoerd moeten worden.

[13] Op basis van publieke bronnen (NCSC, Z-CERT), sectorale informatie (Z-CERT, NVZ, Santeon), informatie van leveranciers en eerdere incidenten.

5.3. Rollen en verantwoordelijkheden

5.3.1. Algemene rollen

Alle medewerkers
Alle medewerkers, iedereen die werkzaam is in het St. Antonius Ziekenhuis en onder het gezag van de organisatie valt, dienen:
- Kennis te nemen van het voorliggende beleid, inclusief de ondersteunende documenten die voor hen relevant zijn[14];
- Zich bewust te zijn van de bijdrage die zij zelf dienen te leveren aan informatiebeveiliging;
- Het beleid toe te passen en niet te omzeilen;
- Te kunnen uitleggen wat de gevolgen zijn van het niet naleven van het beleid voor de voor hen relevante thema's;
- Specifieke verantwoordelijkheden zijn onder meer:
- Onverwijld rapporteren van beveiligingsincidenten (inclusief datalekken);
- Toepassen van algemene beveiligingsmaatregelen (inclusief clean desk/clear screen, het zichtbaar dragen van toegangspassen, het afsluiten van een deur bij het verlaten van een ruimte);
- Volgen van verplichte trainingen m.b.t. gegevensbescherming en informatiebeveiliging;
- Medewerking verlenen aan interne en externe audits en verbeteracties.

Leidinggevenden
Leidinggevenden zijn verantwoordelijk voor het naleven van het informatiebeveiligingsbeleid voor hun afdeling en/of medewerkers.
Leidinggevenden:
- Vervullen een voorbeeldfunctie: zij dragen het beleid zichtbaar uit en ondermijnen het niet;
- Behandelen informatiebeveiliging in werkoverleggen en jaargesprekken;
- Spreken medewerkers erop aan als informatiebeveiligingsregels overtreden worden;
- Treffen maatregelen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen;
- Zorgen voor adequate (continuïteits)maatregelen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden;
- Benoemen binnen hun team(s) in overleg met de CISO, PO en FG de aandachtsvelders en control eigenaren ter ondersteuning van de lokale implementatie van het informatiebeveiligingsbeleid;
- Beschikken over middelen voor het melden en afhandelen van beveiligingsincidenten inclusief vertrouwelijke incidenten;
- Evalueren (de afhandeling van) beveiligingsincidenten om de processen te verbeteren;
- Treffen maatregelen zodat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen;
- Melden grote en/of hoog risico verandertrajecten met een hoog risico op gebied van gegevensbescherming en/of informatiebeveiliging tijdig aan de CISO en FG, nog voor de start van het project;
- Benoemen projectmanagers om trajecten en te leiden en die als contactpersoon dienen voor de CISO, PO en FG.

Projectmanagers
Bij het doorvoeren van wijzigingen in de organisatie, in welke vorm dan ook, moet aandacht zijn voor het beheersen van risico's ten aanzien van patiëntveiligheid, gegevensbescherming en informatiebeveiliging. Uitgangspunten hierbij zijn *"privacy en security by design en default"*: Gegevensbescherming en informatiebeveiliging wordt meegenomen vanaf de planfase van het project en systemen worden standaard veilig geconfigureerd en opgeleverd. Het is de taak van de projectmanagers om dit te borgen.
Projectmanagers zijn verder verantwoordelijk voor:
- Het volgen van de vereiste projectmethodiek inclusief het uitvoeren van BIA's (business impact analyses), DPIA's (data protection impact assessments) en (prospectieve) risicoanalyses;

[14] Het St. Antonius Ziekenhuis stelt hiertoe het beleid in een beknopte versie ter beschikking inclusief een leeswijzer voor de relevante stukken.

- Het tijdig en volledig betrekken van de CISO, PO en FG bij grote en/of hoog risico projecten zodanig dat a) deze beschikken over voldoende informatie om een inschatting te kunnen maken van de risico's met betrekking op gegevensbescherming en informatiebeveiliging; en b) er voldoende tijd en gelegenheid is om gefundeerde keuzes en afwegingen te maken ten aanzien van de beheersing van risico's.
- Het opleveren van documentatie ten behoeve van de staande organisatie zodat deze het resultaat van het project in gebruik kan nemen.

Eigenaren informatiesysteem
Alle systemen hebben een eigenaar. Eigenaren zijn eindverantwoordelijk voor het uitvoeren van informatiebeveiligingsmaatregelen voor dat systeem inclusief:
- Uitvoeren van risicoanalyses;
- Uitvoeren van data protection impact assessments;
- Uitvoeren van business impact analyses;
- Zorgen dat alle verantwoordelijkheden (onderhoud, beheer) zijn belegd.

Indien geen eigenaar benoemd is valt het eigenaarschap terug naar de RvB.

5.3.2. Bestuur en toezicht

Raad van Bestuur (RvB)
De Raad van Bestuur is eindverantwoordelijk voor alle activiteiten binnen de organisatie en hiermee ook voor gegevensbescherming en informatiebeveiliging. De verantwoordelijkheid omvat onder andere het vaststellen van het gegevensbescherming en informatiebeveiliging beleid, het bepalen van het acceptabele risiconiveau (de risicobereidheid) en het mede uitdragen van het belang van gegevensbescherming en informatiebeveiliging binnen de organisatie. Binnen de RvB is de Chief Financial Officer (CFO) portefeuillehouder gegevensbescherming en informatiebeveiliging. De CFO beoordeelt investeringsaanvragen van de manager ARC ten behoeve van gegevensbescherming en informatiebeveiliging. De RvB zorgt voor voldoende middelen om de doelstellingen ten aanzien van gegevensbescherming en informatiebeveiliging te behalen. Ook stelt de RvB de wettelijk verplichte functionarissen aan zoals de FG.

Raad van Toezicht (RvT)
De Raad van Toezicht toetst of de Raad van Bestuur haar verplichtingen ten aanzien van gegevensbescherming en informatiebeveiliging nakomt inclusief het voldoen aan de relevante wet- en regelgeving.

Internal auditors
De internal auditors van de afdeling AR&C:
- Zijn verantwoordelijk voor het onderhouden van het interne audit programma voor NEN 7510 en ISO 27001;
- Stellen in overleg met CISO, PO en FG het interne audit programma vast conform vereisten zodat:
- Alle NEN 7510 en ISO 27001 maatregelen minimaal 1x in de drie jaar worden geaudit.
- Alle vestigingen minimaal 1x in de drie jaar worden geaudit.
- Toetsen aan de NEN 7510 en ISO 27001 normen en nemen eerdere bevindingen mee bij de audits.

Ondernemingsraad
De ondernemingsraad ziet toe op de uitvoerbaarheid en uitvoering van het gegevensbescherming en informatiebeveiliging beleid en relevante wet- en regelgeving vanuit het oogpunt van de werknemers.

5.3.3. ICT Governance

IBO (Informatiebesturingsoverleg)
Het IBO bepaalt de IT visie en strategie binnen het ziekenhuis, rekening houdend met gestelde randvoorwaarden en beleid op het gebied van gegevensbescherming en informatiebeveiliging.

IV Raad (Informatievoorziening)
De IV Raad is verantwoordelijk voor de vertaalslag van de visie en strategie van het ziekenhuis en specifiek I&I naar het projectportfolio, en delegeert deze verantwoordelijkheid naar de domeinen.

EISC (Enterprise Information Steering Committee)
De EISC prioriteert binnen de strategische kaders over de op te leveren informatieproducten en ziet toe op een zinvol portfolio van rapporten en dashboards.

Domeinen
Informatiesystemen zijn onderverdeeld in vijf domeinen: Zorg, Beeldvorming & Diagnostiek, Bedrijfsvoering & Zorglogistiek, Kennis en Keten.
Elk domein heeft een domeineigenaar die de portefeuille binnen hun aandachtsgebied bewaakt en impact overziet van de projecten op de organisatie en zorgprocessen. Domeineigenaren vervullen samen met de Informatiemanagers en de Medisch Ambassadeurs een belangrijke rol in het tot stand komen van het I&I Project Portfolio en zien toe op de uitvoering van risicoanalyses.

5.3.4. Individuele rollen en functionarissen

Chief Medical Information Officer (CMIO)
De CMIO houdt zich bezig met de doorontwikkeling van ICT op strategisch en tactisch niveau. Hij heeft een stem in de prioritering, planvorming en besluitvorming. Hierbij vertegenwoordigt de CMIO de medisch specialisten bij de verbetering en doorontwikkeling van het EPD en andere medisch-ondersteunende systemen.

Chief Nursing Information Officer (CNIO)
De CNIO houdt zich bezig met de doorontwikkeling van ICT op strategisch en tactisch niveau en heeft een belangrijke stem in de prioritering, planvorming en besluitvorming. Hierbij vertegenwoordigt de CNIO de collega's in het verpleegkundig vakgebied en andere gebruikersgroepen, zoals de polimedewerkers.

Manager Mens en Organisatie
De manager Mens en Organisatie (voorheen HR en M&C) is verantwoordelijk voor het opstellen en uitvoeren van het personeelsbeleid inclusief relevante aspecten voor informatiebeveiliging waaronder screening van medewerkers, mutaties in het personeelsbestand en het vaststellen van het disciplinaire proces bij ernstige overtredingen door medewerkers. De Eenheid borgt dat arbeidsovereenkomsten en gastovereenkomsten eisen tot geheimhouding en naleving van de gedragscode (waaronder het beleid gegevensbescherming informatiebeveiliging) bevatten. Ten aanzien van marketing en communicatie zorgt de manager voor de beschikbaarheid van een M&C-adviseur en/of –medewerker om I&I advies te geven bij marketing en/of communicatievraagstukken op het gebied van informatiebeveiliging. Afhankelijk van gevraagde hulp en bijbehorende benodigde capaciteit verleent de eenheid kosteloos (reguliere adviezen en communicatieactiviteiten) dan wel tegen betaling (grotere adviestrajecten of campagnes) diensten aan I&I voor advies en uitvoering van M&C-activiteiten.

Manager Diagnostiek en Medische Technologie
De manager bedrijfsvoering en medisch manager Diagnostiek en Medische Technologie zien toe op de aanschaf en beheer van medische apparatuur. Overeenkomstig de verantwoordelijkheden van de leidinggevenden en projectmanagement betrekken zij de PO, CISO, ISO en FG bij nieuwe projecten.

Manager Inkoop en Facilitaire Zaken
De manager Inkoop en Facilitaire Zaken is eindverantwoordelijk voor:
- Het uitvoeren van het fysieke beveiligingsbeleid voor de locaties;
- Het borgen van de continuïteit van de bedrijfsvoering in relatie tot fysieke beveiliging en nutsvoorzieningen.

Wanneer de organisatie diensten (of producten) afneemt of samenwerkingsverbanden aangaat met externe partijen moet dit gebeuren in overeenstemming met het geldende Inkoopbeleid en toepasselijke wet- en regelgeving. De Manager Inkoop en Facilitaire Zaken legt het beleid vast.

Afdelingshoofd Juridische Zaken
De jurist:
- Signaleert proactief en adviseert de RvB, leidinggevenden, beroepsbeoefenaren en medische staf over alle voor het ziekenhuis relevante rechtsgebieden waaronder contractenrecht, aansprakelijkheid en verzekeringen, (medisch) straf- en tuchtrecht, aanbestedingsrecht en gezondheidsrechtelijke vraagstukken;
- Toetst contracten aan relevante wet- en regelgeving en beleid;
- Is vast aanspreekpunt voor betrokken beroepsbeoefenaren, belangenbehartigers, advocaten en andere relevante partijen;
- Is verantwoordelijk voor het onderhouden van relevante netwerken zowel binnen als buiten de organisatie.

5.3.5. Gegevensbescherming en informatiebeveiliging functionarissen

Corporate Information Security Officer (CISO)
De CISO heeft een rol op strategisch niveau. Hij rapporteert aan de manager AR&C, maar is zelf geen lijnverantwoordelijke. Zijn voornaamste taak is te waken over informatiebeveiliging in de organisatie. Bij eventuele wetswijzigingen brengt de CISO de impact hiervan in kaart en brengt hij advies uit aan de manager ARC over eventuele noodzakelijk te nemen acties of maatregelen. Hoewel de CISO primair het informatiebeveiligingsbeleid opstelt, betekent dit niet dat de CISO voor alle onderdelen uit de NEN 7510 primair verantwoordelijk is. Bijlage 3 geeft voor alle hoofdstukken van de NEN 7510 en ISO 27001 aan wie hoofdverantwoordelijk is. De exacte verantwoordelijkheden per beheersmaatregel worden door de CISO in overleg vastgesteld.
De CISO:
- Stelt samen met de PO het gegevensbescherming- en informatiebeveiligingsbeleid op;
- Is verantwoordelijk voor de inrichting van het managementsysteem voor informatiebeveiliging (Information Security Management System of ISMS);
- Geeft op verzoek of uit eigen initiatief advies aan de manager AR&C en RvB over informatiebeveiliging;
- Stelt samen met de PO en FG de directiebeoordeling en andere rapportages op;
- Coördineert het security awareness programma;
- Vertegenwoordigt de organisatie naar buiten toe op het gebied van informatiebeveiliging;
- Ziet toe op de selectie en ingebruikname van informatiesystemen, zowel intern als extern;
- Adviseert in geval van crisis in samenspraak met betrokkenen;
- Is bevoegd tot het (laten) uitvoeren van gap- en risicoanalyses;
- Leidt na ernstige ziekenhuisbrede informatiebeveiligingsincidenten het uitvoeren van oorzaakanalyses;
- Onderhoudt contacten met speciale belangengroepen;
- Richt het control framework programma in;
- Is strategisch contactpersoon voor Z-CERT en NVZ (voor informatiebeveiliging)
- Vervangt de FG bij afwezigheid.
- Adviseert aan de bestuursadviescommissie gegevensbescherming en informatiebeveiliging.

Functionaris Gegevensbescherming (FG)
Op grond van de AVG is in het ziekenhuis een FG aangesteld die de taak heeft om intern toezicht te houden op de toepassing en naleving van de AVG en de Raad van Bestuur. De FG kan aan de organisatie een onafhankelijk oordeel verschaffen over deze naleving en/of hierover adviseren. De FG:
- Ziet toe op de implementatie van de Algemene Verordening Gegevensbescherming (AVG) inclusief de gegevensuitwisseling met derden
- Toetst periodiek en onafhankelijk of adequate maatregelen zijn getroffen om risico's te beheersen, in samenwerking met internal audit;
- Is contactpersoon voor de AP;
- Adviseert de RvB;
- Vervangt de CISO bij afwezigheid.[15]

[15] De FG is onafhankelijk, maar naar gelang de inrichting van de organisatie kan de RvB besluiten deze rol te combineren met andere rollen. Het uitgangspunt is dat de invulling van de FG rol bij escalaties prioriteit heeft vóór

Privacy Officer (PO)
De privacy officer[16]:
- Stelt samen met de CISO het gegevensbescherming- en informatiebeveiligingsbeleid;
- Is verantwoordelijk voor het opstellen en actueel houden van de privacyverklaring;
- Adviseert de organisatie over beleid, processen en protocollen;
- Adviseert zowel de organisatie als externe personen (patiënten, medewerkers etc.) bij privacyvraagstukken;
- Adviseert over het uitvoeren van DPIAs en verwerkersovereenkomsten;
- Onderhoudt de registers voor gegevensverwerkingen en datalekken;
- Meldt datalekken bij de AP;
- Bevordert de bewustwording op het gebied van de bescherming van persoonsgegevens;
- Is bevoegd tot het (laten) uitvoeren van gap- en risicoanalyses en logcontroles.

Assistent Functionaris Gegevensbescherming
De Assistent Functionaris Gegevensbescherming:
- Ondersteunt de Privacy Officer (PO) en Functionaris Gegevensbescherming (FG) bij hun werkzaamheden en taken binnen het ziekenhuis, inclusief het inschatten van en zelfstandig adviseren over vragen, problemen en risico's op het gebied van gegevensbescherming binnen de organisatie en datalekken;
- Onderhoudt de registers voor interne en externe gegevensverwerkingen;
- Coördineert de afhandeling van de datalekmeldingen in de organisatie.

Information Security Officer (ISO)
Afdelingen met een specifieke verantwoordelijkheid voor informatiebeveiliging (zoals de afdeling I&I) kunnen een voltijd Information Security Officer aanstellen die actief is op tactisch en operationeel niveau.

Aandachtsvelders
Aandachtsvelders zijn medewerkers op een afdeling met specifieke interesse en/of kennis op het gebied van gegevensbescherming en informatiebeveiliging. Zij worden door hun leidinggevende aangewezen als aandachtsvelder en ondersteunen de PO en CISO bij de uitvoering van het beleid en fungeren als "champion".
Deze lokale verantwoordelijken hebben onder meer de volgende taken:
- Uitdragen van het gegevensbescherming en informatiebeveiliging beleid en zorgen voor bewustwording bij collega's;
- Mede-implementeren en borgen van het gegevensbescherming en informatiebeveiliging beleid op de afdeling;
- Beantwoorden van vragen van medewerkers van de afdeling over gegevensbescherming en informatiebeveiliging;
- (Helpen bij) het melden van informatiebeveiligingsincidenten en datalekken;
- Assisteren bij acties die voortvloeien uit informatiebeveiligingsincidenten en datalekken;
- Uitvoeren van beheersmaatregelen zoals afgesproken met de CISO en de leidinggevende.

Manager afdeling Audit, Risk en Compliance (AR&C)
De manager Audit, Risk en Compliance (AR&C) verzorgt de normale communicatie over gegevensbescherming en informatiebeveiliging naar de RvB. De Manager AR&C:
- Is budgeteigenaar voor gegevensbescherming en informatiebeveiliging;
- Stelt het AR&C jaarplan op.

Coördinator Risicomanagement en Compliance
De compliance coördinator (onderdeel van de Bestuursstaf van de RvB) onderhoudt:
- De lijst met relevante wet- en regelgeving voor de organisatie;
- Een lijst met integrale risico's in het kader van integraal risicomanagement (IRM), waarvan informatiebeveiliging onderdeel uitmaakt.

---

eventuele andere rollen. In gevallen waar er mogelijke belangenconflicten tussen deze rollen zijn kan de RvB als wenselijk intern bij juridische zaken advies inwinnen of extern bij een deskundige.
[16] De Privacy officer is een rol die bij één of meerdere personen kan worden belegd.

Control eigenaren
Een control eigenaar is eindverantwoordelijk voor de implementatie van een beheersmaatregel (zoals gedefinieerd in NEN 7510 en ISO 27001 of anders vastgesteld door de CISO). Een control eigenaar levert bewijs aan dat de beheersmaatregel aantoonbaar is geïmplementeerd. Dit gebeurt met een bepaalde frequentie vastgesteld door de CISO. Control eigenaren worden benoemd door de leidinggevende die eindverantwoordelijk is voor de beheersmaatregel. Een control eigenaar kan zijn/haar taak delegeren naar één of meer control uitvoerders.

Control uitvoerder
Een control uitvoerder voert beheersmaatregelen uit zoals afgesproken met de control eigenaar.

5.3.6. ICT-specifieke rollen

Chief Information Officer (CIO)
De CIO is eindverantwoordelijk voor de centrale geautomatiseerde informatievoorziening inclusief:
- De aantoonbare uitvoer van informatiebeveiligingsbeheersmaatregelen door I&I;
- De beveiliging van de centrale ICT-infrastructuur conform het beveiligingsbeleid;
- Het uitvoeren van algemene servicemanagementprocessen ten behoeve van de stabiliteit en continuïteit van de dienstverlening;
- Het aanvragen van voldoende middelen bij de RvB om informatiebeveiliging en continuïteit te borgen.

I&I Information Security Officer (ISO)
De ISO is actief op tactisch en operationeel niveau voor de eenheid I&I. De ISO:
- Is voorzitter van het Computer Security Incident Response Team;
- Participeert in projecten voor wijziging, ingebruikname of beëindiging van systemen;
- Is bevoegd tot het (laten) uitvoeren van gap- en risicoanalyses;
- Ondersteunt waar nodig de leidinggevenden bij informatiebeveiligingsvraagstukken;
- Onderhoudt contacten met speciale belangengroepen;
- Is tactisch contactpersoon voor Z-CERT.

Enterprise Architect (EA)
De EA geeft inzicht in en houdt samen met eigenaren regie op het ICT landschap inclusief de informatiestromen en de interfaces daarvan, zowel in de eigen organisatie als naar en van andere organisaties.

Informatiemanagers
Informatiemanagers zijn de verbindende schakel tussen I&I en de overige organisatieonderdelen. De informatiemanagers:
- Zijn op strategisch en tactisch niveau betrokken bij het opstellen van de jaarplannen en de (voorgenomen) RvB besluiten van de diverse organisatieonderdelen;
- Toetsen deze jaarplannen en besluiten tegen het vigerende beleid op het gebied van gegevensbescherming en informatiebeveiliging en technische mogelijkheden;
- Zijn direct of indirect (in overleg met een informatieadviseur) het aanspreekpunt voor de introductie van nieuwe systemen en het wijzigen of uitfaseren van bestaande systemen;
- Betrekken overeenkomstig de verantwoordelijkheden van leidinggevenden en projectmanagers (zie pagina 25) de PO, CISO, ISO en/of FG tijdig bij nieuwe initiatieven.

Informatieadviseurs
Informatieadviseurs zijn de verbindende schakel tussen de Informatiemanagers en de informatiesysteemeigenaren, beheerders en gebruikers. De informatieadviseurs:
- Zijn het aanspreekpunt voor het uitvoeren van de projecten van nieuwe systemen en het wijzigen of uit faseren van bestaande systemen;
- Vertalen de uitkomsten van de Business Impact Analyse naar concrete systeemvereisten;
- Werken samen met de betrokken leverancier, deskundige van het informatiesysteem, beheerders en gebruikers om deze systeemvereisten te implementeren.

Afdelingshoofd IT Operations
Het afdelingshoofd IT operations is verantwoordelijk voor de beveiliging van de infrastructuur (netwerken, systemen, opslag) en het technisch applicatiebeheer overeenkomstig het informatiebeveiligingsbeleid. Dit betreft onder meer:
- Hardening van systemen;
- Beheersing van technische kwetsbaarheden (patchen).

Het Afdelingshoofd is tevens verantwoordelijk voor de technische beveiliging van de werkplekken en het aansturen van de teams werkplekondersteuning, Helpdesk, CVT en functioneel applicatiebeheerders zodat zij werken conform het informatiebeveiligingsbeleid.
De ICT Helpdesk:
- Registreert en behandelt (potentiële) informatiebeveiligingsincidenten inclusief datalekken;
- Beoordeelt binnengekomen tickets op legitimiteit volgende geldende procedures alvorens deze uit te laten voeren.

Functioneel beheerders
Een functioneel beheerder ondersteunt de informatiesysteemeigenaar bij het bepalen van de inrichting van het systeem, inclusief de inrichting van informatiebeveiliging zoals rollen en autorisaties.

Applicatiebeheerder / databasebeheerder
De applicatiebeheerder verzorgt operationele instandhouding van het informatiesysteem / gegevensverzameling en ziet toe op een juiste werking hiervan.

Technisch beheerder
Een technisch beheerder verzorgt de technische infrastructuur van een informatiesysteem inclusief hardening en patching.

Gebruiker
Een gebruiker is iemand die gebruik maakt van een informatiesysteem. Iedere gebruiker volgt het specifieke beleid dat van toepassing is op dat informatiesysteem.

5.3.7. Wetenschappelijk onderzoek
Ten behoeve van gegevensverwerkingen voor (medisch) wetenschappelijk onderzoek en kwaliteitsregistraties zijn specifiek afspraken gemaakt met de afdeling Research & Development (R&D). Deze afspraken zijn vastgelegd in de Privacyrichtlijn wetenschappelijk onderzoek en komen erop neer dat alle onderzoeken lokaal worden getoetst.

METC en de Lokale Toetsingscommissie
De METC en de Lokale Toetsingscommissie hebben elk een eigen verantwoordelijkheid voor het toetsen en goedkeuren van gegevensverwerkingen voor (medisch) wetenschappelijk onderzoek. Aangezien voor deze onderzoeken uitwisseling (doorgiften) van gegevens vaak essentieel is (zeker indien wordt samengewerkt met andere zorgaanbieders of onderzoekers), zijn specifiek afspraken vastgelegd in het beleid gegevensuitwisseling voor kwaliteitsregistraties en wetenschappelijk onderzoek.

5.3.8. Externen

Leveranciers
Leveranciers dienen informatiebeveiligingsincidenten die bij hen plaatsvinden inclusief datalekken en kwetsbaarheden tijdig te communiceren aan het St. Antonius Ziekenhuis en zich (conform vastgelegde afspraken) te conformeren aan het informatiebeveiligings- en gegevensbeschermingsbeleid van het St. Antonius Ziekenhuis. Indien medewerkers van leveranciers directe toegang hebben tot systemen van het St. Antonius Ziekenhuis moet de leverancier het St. Antonius Ziekenhuis tijdig op de hoogte te stellen van relevante mutaties in het personeelsbestand.

Externen
Externen (studenten, vrijwilligers, gasten, bezoekers en externe relaties) die ingezet worden voor taken in de organisatie of gebruikmaken van diensten dienen zich, voor zover van toepassing, te houden aan het informatiebeveiligingsbeleid.

Externe auditors
De externe auditors zorgen voor een onafhankelijke beoordeling van de informatiebeveiliging van het St. Antonius Ziekenhuis.

Externe accountant
De externe accountant ziet toe op de implementatie van algemene IT beheersmaatregelen (IT Generic Controls of ITGC) ten behoeve van de financiële verslaglegging.

5.4. Gegevensregisters

Binnen het ziekenhuis houden we diverse registers bij in relatie tot de verwerking van persoonsgegevens. Op grond van de AVG houden we een centraal verwerkingsregister en een datalekkenregister bij. In het verwerkingsregister is tevens een overzicht te raadplegen van de applicaties (software)systemen) die we gebruiken voor de gegevensverwerkingen. Daarnaast houden we nog een specifiek register bij met maatregelen die we in het kader van grensoverschrijdend gedrag door patiënten en/of bezoekers hebben opgelegd. Het ziekenhuis houdt ook registers bij op grond van de Wkkgz, zoals het VIM-register of calamiteitenregister, maar deze worden niet in dit document besproken.

5.4.1. Verwerkingsregister

We zijn als ziekenhuis verplicht al onze verwerkingen te registreren. Dit betreft zowel verwerkingen die we volledig binnenshuis afhandelen als verwerkingen waarvoor we een andere partij (de 'verwerker') inschakelen. Ook de minimale informatie die in zo'n register moet worden opgenomen, is in de AVG vastgelegd. Dit betreft:

- De naam en contactgegevens van de verwerkingsverantwoordelijke, eventueel de gezamenlijke verwerkingsverantwoordelijken (bijvoorbeeld ziekenhuis en MSB) en FG;
- De doelen van de verwerking (dit betreft de specifieke doelen per verwerking);
- De categorieën persoonsgegevens en de daarbij behorende categorieën betrokkenen;
- De categorieën ontvangers van de persoonsgegevens (ook ontvangers in derde landen);
- Doorgifte van persoonsgegevens aan een derde land of internationale organisatie (met vermelding van het land of die organisatie);
- Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën persoonsgegevens moeten worden gewist;
- Indien mogelijk, een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen.
- De wettelijke grondslag van de verwerking[17]

Naast deze verplichte gegevens, leggen we in ons verwerkingsregister ook vast:

- Wie de intern verantwoordelijke is;
- Wie toegang hebben tot de gegevens (alleen bij volledig interne verwerkingen);
- Indien van toepassing, wie de verwerker is;
- Welke software applicatie(s) gebruikt wordt voor de betreffende gegevensverwerking;
- Of er een risicoanalyse is uitgevoerd.

Het verwerkingsregister bestaat uit een database in ons Kwaliteitsnet en wordt centraal bijgehouden. Elke intern verantwoordelijke rapporteert aan de FG over de verwerkingen zodat deze centraal inzichtelijk zijn. Indien er sprake is van een verwerker, wordt het formulier tezamen met de verwerkersovereenkomst toegestuurd en geregistreerd. Het ziekenhuis hanteert in beginsel en bij voorkeur de standaard verwerkersovereenkomst van de Brancheorganisaties Zorg (BOZ). Deze overeenkomst moet tezamen met de hoofdovereenkomst altijd te worden gecontroleerd door de (assistent-)FG. Zie voor een beschrijving van de werkwijze ook het beleidsdocument Verwerkersovereenkomst - Checklist wel of niet noodzakelijk.

5.4.2. Datalekkenregister

Indien er inbreuken plaatsvinden met persoonsgegevens dienen deze te worden geregistreerd en gedocumenteerd. De Autoriteit Persoonsgegevens (AP) kan op basis van die informatie controleren of

[17] indien dit "gerechtvaardigd belang" is wordt ook vastgelegd welke afwegingen hierbij zijn gemaakt – zie het kader in Bijlage 3 - Afwegingskader grondslag gerechtvaardigd belang.

het ziekenhuis zich aan de regels met betrekking tot datalekken houdt. De registratie vindt automatisch plaats doordat een melder van een inbreuk het formulier ‘melding datalek’ moet invullen (paragraaf 4.4).

5.4.3. Register met waarschuwingen, gele en rode kaarten

Helaas hebben we in het ziekenhuis met enige regelmaat te maken met patiënten en/of bezoekers die zich grensoverschrijdend gedragen. Dat kan verbaal zijn (zoals onheuse bejegening, schelden, dreigen), maar ook fysiek (zoals agressief gedrag). Ter bescherming van de veiligheid van alle patiënten en medewerkers hanteren we) daarom beleid en maatregelen om dit gedrag zoveel mogelijk te voorkomen of bij te sturen. Indien dezelfde patiënt en/of bezoeker vaker of zeer ernstig grensoverschrijdend gedrag vertoond, kan dit leiden tot een waarschuwing, een gele of rode kaart. De persoonsgegevens en de opgelegde maatregel leggen we vast in een register. Deze gegevens worden in principe maximaal één jaar bewaard.

6. Uitvoering gegevensverwerkingen

In dit hoofdstuk beschrijven we de meer specifieke verwerking van persoonsgegevens.[18]

6.1. Primair proces (zorg)

Voor het primaire proces worden patiëntgegevens verwerkt. Patiënten zijn alle personen aan wie (of voor wie in het geval van consultatie) het St. Antonius zorg verleent. Tegenwoordig is dat niet alleen de zorg op locatie in het ziekenhuis, maar ook zorg op afstand, zoals telemonitoring. De gegevens die verwerkt worden, zijn noodzakelijk om goede zorg en nazorg te verlenen, zorgprocessen te organiseren en om de zorgverlening bedrijfsmatig af te handelen. Het betreft identificerende gegevens zoals naam, geslacht, geboortedatum, BSN- en paspoortnummer, foto's, contactgegevens, verzekeringsgegevens, medische gegevens, genetische gegevens en etnische en seksuele gegevens (voor zover van belang voor de zorgverlening). Behalve voor het primaire proces kunnen de gegevens of een deel daarvan ook gebruikt worden voor (wetenschappelijk) onderzoek, een claim- en klachtenafhandeling of een gerechtelijke procedure.

Indien patiënten een rechtsgeldig vertegenwoordiger hebben (bijvoorbeeld mentoren of familieleden), dan worden ook de gegevens van deze personen in het patiëntendossier verwerkt. Het gaat dan om namen en contactgegevens en - indien van toepassing - aanstellingsbrieven van de rechtbank.

Daarnaast kunnen hun gegevens worden verwerkt indien zij betrokken zijn bij een klacht. De klachtenfunctionarissen houden daartoe zelf dossiers en bestanden bij. Deze worden niet met anderen gedeeld dan ten behoeve van de klachtafhandeling.

Ook als andere zorgverleners betrokken zijn bij de behandeling van de patiënt, worden hun gegevens in het dossier verwerkt. Dit geldt standaard voor huisartsen (als zijnde verwijzers van de patiënt), maar ook voor betrokken zorgverleners van andere zorginstellingen of zorgverleners die in consultatie worden geroepen.

De bewaartermijn van de patiëntgegevens is conform WGBO 20 jaar na de laatste wijziging in het patiëntendossier. Gegevens worden eventueel langer bewaard indien dat nodig is vanuit het oogpunt van goed hulpverlenerschap of voor wetenschappelijk onderzoek.

Behalve verwerking van gegevens in onze eigen systemen, worden patiëntgegevens ook verwerkt (bijvoorbeeld uitgewisseld) met andere zorgverleners. Dit kan het geval zijn als een patiënt wordt doorverwezen, als er sprake is van ketenzorg of als een deel van de zorg wordt uitbesteed. Daarnaast heeft het ziekenhuis voor diverse verwerkingen externe verwerkers ingeschakeld. Ook zij ontvangen en verwerken in opdracht van het ziekenhuis patiëntgegevens.

6.2. Bedrijfsvoering (medewerkers, financiële zaken, kwaliteitsbewaking, e.d.)

In het ziekenhuis zijn er behalve directe zorgverlening tal van andere bedrijfsprocessen, zoals personeelsbeleid, scholing, kwaliteitsontwikkeling, financiële administratie, logistieke zaken, juridische zaken, marketing, databeheer, etc. Voor al deze processen worden gegevens verwerkt van zowel patiënten als medewerkers en van externe leveranciers en dienstverleners.

6.2.1. Patiënten

Door de behandelingsovereenkomst met en zorgverlening aan patiënten beschikt het ziekenhuis over uitgebreide informatie en persoonsgegevens van deze patiënten. Een deel van deze gegevens is tevens nodig voor de bedrijfsmatige organisatie van de zorg (bijvoorbeeld financiën). De gegevens die daarvoor verwerkt worden zijn met name identificerende gegevens en gegevens over de verleende zorg. Daarnaast is gegevensverwerking nodig voor de bewaking van de kwaliteit en veiligheid van zorg binnen het ziekenhuis. Daartoe worden persoonsgegevens over het zorgproces en de uitkomsten daarvan verwerkt. Het doel van de verwerking kan algemene kwaliteitsverbetering betreffen

[18] NB: voor de verwerkingen genoemd in dit hoofdstuk moet aan alle voorwaarden van de AVG en WGBO te worden voldaan zoals beschreven in het vorig hoofdstuk (o.a. rechtvaardige grondslag, minimale bewaartermijn, etc.)

(bijvoorbeeld door verplichte landelijke kwaliteitsregistraties), maar kan ook direct te maken hebben met een onderzoek naar incidenten of calamiteiten bij de zorgverlening in het ziekenhuis.

6.2.2. Medewerkers

In relatie tot het werkgeverschap en de administratieplicht van het ziekenhuis worden van medewerkers identificerende gegevens verwerkt zoals naam, geslacht, nationaliteit, geboortedatum, BSN-nr., kopie ID-bewijs, foto's, contactgegevens, bankgegevens en gegevens betreffende de bevoegdheid van medewerkers (BIG-registratie, diploma's en VOG). Daarnaast worden gezondheidsgegevens verwerkt in verband met de screening op gezondheidsrisico's ter bescherming van onze patiënten en medewerkers. De bewaartermijn van deze gegevens is 7 jaar.

Voor een goede uitvoering van het personeelsbeleid is het noodzakelijk dat gegevens worden verwerkt over het functioneren van medewerkers. Dit betreft onder meer gegevens over scholing, persoonlijke ontwikkelingsplannen, verslagen van functioneringsgesprekken, verzuim en reïntegratieplannen en disciplinaire maatregelen zoals bijvoorbeeld waarschuwingen. Deze gegevens worden alleen verwerkt door leidinggevenden van de medewerker en worden gedurende het gehele dienstverband bewaard, met uitzondering van jaargespreksverslagen. Hiervoor geldt tijdens het dienstverband een bewaartermijn van 10 jaar. Na afloop van het dienstverband worden gegevens nog gedurende de termijn bewaard.
Indien noodzakelijk worden gegevens van medewerkers ook verwerkt in arbeidsrechtelijk procedures.

Aangezien het ziekenhuis met veel externe partijen samenwerkt, is het in die gevallen ook noodzakelijk om gegevens van medewerkers aan deze partijen te verstrekken. Dit zijn echter altijd werkgerelateerde gegevens en alleen in specifieke gevallen en met toestemming van de medewerker privégegevens zoals een tel.nr., adres of e-mailadres (bijv. voor de bedrijfsarts). Van medewerkers van deze externe partijen verwerkt het ziekenhuis zelf ook gegevens, met name contactgegevens. Ook voor de verwerking van gegevens van medewerkers worden externe verwerkers ingeschakeld.

6.2.3. Sollicitanten

Ten behoeve van de selectieprocedure van nieuwe medewerkers wordt van sollicitanten een beperkter aantal gegevens verwerkt. Dit betreft alleen de gegevens die noodzakelijk zijn om contact te onderhouden met de sollicitant en om te verifiëren of een sollicitant aan kwalificaties voldoet. Het betreft identificerende gegevens zoals naam, geslacht, geboortedatum, contactgegevens, gegevens betreffende de loopbaan van de sollicitant (CV) en de bevoegdheid van de sollicitant (BIG-registratie en diploma's). Gegevens die de sollicitant zelf op zijn CV zet (bijvoorbeeld huwelijkse staat), zullen derhalve ook verwerkt worden. Pas als een sollicitant wordt aangenomen, worden de overige noodzakelijke gegevens (zoals beschreven bij medewerkers) verwerkt.

Als een sollicitant wordt afgewezen maar akkoord gaat met het bewaren van zijn gegevens, worden de gegevens nog een jaar lang bewaard. In andere gevallen worden de gegevens van afgewezen sollicitanten binnen vier weken na het einde van de sollicitatieprocedure vernietigd.

6.2.4. Raad van Toezicht, cliëntenraad en vrijwilligers

Leden van de Raad van Toezicht (RvT) en cliëntenraad vallen niet onder de groep medewerkers, maar zijn wel onderdeel van de ziekenhuisorganisatie. Van hen worden de namen, foto's, geslacht, contactgegevens en bankgegevens verwerkt. Van RvT-leden worden ook hun reguliere functies en nevenactiviteiten verwerkt, evenals de vergoeding die zij voor hun toezichtstaak ontvangen. Van vrijwilligers worden alleen naam, geslacht, contactgegevens en bankgegevens verwerkt.

6.3. (Wetenschappelijk) Onderzoek

Het St. Antonius Ziekenhuis is een ambitieus ziekenhuis dat continu wil verbeteren. We leveren zorg vanuit de persoonlijke behoefte van de patiënt en handelen daarbij op basis van recente en innovatieve bevindingen. Ook door zelf onderzoek te doen, dragen wij hieraan bij. De uitkomsten van onderzoek gebruiken we voor onze zorgverlening. We investeren daarom in onderwijs (zie volgende paragraaf), onderzoek en de ontwikkeling van onze medewerkers. Om goed onderzoek te doen, is het noodzakelijk persoonsgegevens te verwerken. Afhankelijk van het type onderzoek wordt bepaald welke gegevens nodig zijn. Veelal betreft het gegevens over het inhoudelijk zorgproces, medicijngebruik, bepaalde kenmerken van de patiënt en andere relevante gegevens. Uitgangspunt

voor het gebruik van patiëntgegevens voor bepaald (wetenschappelijk) onderzoek is toestemming. Patiënten worden van tevoren specifiek geïnformeerd over het onderzoek en dienen toestemming te geven voor het gebruik van hun persoonsgegevens. Dit geldt ook voor onderzoek dat niet goedgekeurd hoeft te worden door de METC[19]. Op grond van wettelijke bepalingen is een uitzondering mogelijk en kan van dit uitgangspunt worden afgeweken. Dat geldt alleen voor retrospectief onderzoek. De voorwaarden voor deze uitzondering zijn uitgewerkt in de AVG, UAVG en WGBO en komt er kortweg op neer dat onder een '*geen bezwaar systeem'* data gebruikt kan worden mits er wordt voldaan aan alle voorwaarden. De voorwaarden zijn uitgewerkt in zogenaamde uitzonderingsregels die verder gespecificeerd zijn in de interne privacyrichtlijn voor wetenschappelijk onderzoek. De onderzoeker (aanvrager van persoonsgegevens) moet dan voldoende aannemelijk maken dat aan die gestelde voorwaarden wordt voldaan. Voor uitgebreide beschrijving van de werkwijze bij wetenschappelijk onderzoek verwijzen we naar de Privacyrichtlijn wetenschappelijk onderzoek.
NB: een andere mogelijkheid blijft natuurlijk om gebruik te maken van volstrekt anonieme gegevens.

6.4. Opleidingen

Om als ziekenhuis de ambitie waar te maken continu te verbeteren, investeren we als vanzelfsprekend in opleidingen van onze medewerkers. We zijn een lerende organisatie en bieden via de St. Antonius Academie diverse opleidingen. Dit varieert van op maat gemaakte bedrijfsopleidingen tot medisch onderwijs voor verpleegkundigen, coassistenten, arts-assistenten en medisch specialisten. De St. Antonius Academie verwerkt daartoe persoonsgegevens van medewerkers, maar ook van studenten[20]. Het betreft met name identificerende gegevens, gegevens over hun vooropleiding.

6.5. Veiligheid

Patiënten en medewerkers moeten erop kunnen vertrouwen dat ze in een veilige omgeving behandeld worden of werkzaam zijn. Ongewenst en onveilig gedrag door andere patiënten, medewerkers of bezoekers proberen we zoveel mogelijk te voorkomen. Dat betreft niet alleen agressief gedrag, maar ook diefstal, beschadiging van eigendommen, e.d. We maken vanuit dit oogpunt dan ook gebruik van cameratoezicht. Dit gebeurt met name op publieke locaties in en buiten ziekenhuis. Ook op afdelingen wordt soms cameratoezicht gehanteerd indien dit noodzakelijk is voor de bescherming van patiënten en medewerkers en andere middelen niet (voldoende) bijdragen (bijvoorbeeld op de SEH). Voor elke verwerking met cameratoezicht moet het desbetreffende specifieke beleid te worden gevolgd en moet advies te worden gevraagd aan de FG.

6.6. MSB, Santeon en overige samenwerkingen en samenwerkingsverbanden

Het St. Antonius Ziekenhuis werkt nauw samen met diverse ketenpartners. Voor de directe zorgverlening wordt bijvoorbeeld samengewerkt met huisartsen, andere ziekenhuizen en zorgverleners. Ook in het kader van de bedrijfsvoering vindt samenwerking plaats, bijvoorbeeld op het gebied van werving & selectie of inhuur van personeel. Voor deze samenwerkingen is het noodzakelijk persoonsgegevens uit te wisselen. Voor de zorg betreft dit patiëntgegevens en gezondheidsgegevens (zie ook bij primair proces), voor de bedrijfsvoering betreft dit over het algemeen contactgegevens van medewerkers. De gegevensverwerking met deze partijen krijgt pas vorm als het voldoet aan de voorwaarden zoals in dit document verwoord (geldige grondslag, specifiek doel, minimale gegevensverwerking, etc.).

6.6.1. Coöperatief Medisch Specialistisch Bedrijf

De belangrijkste samenwerkingspartner voor de zorgverlening in het ziekenhuis is het Coöperatief Medisch Specialistisch Bedrijf (MSB). Dit bedrijf bestaat uit de vrijgevestigd medisch specialisten werkzaam in ons ziekenhuis en medewerkers die zij zelf in dienst hebben genomen. Het ziekenhuis en het MSB zijn gezamenlijk verantwoordelijk voor de verwerking van persoonsgegevens ten behoeve van de zorgverlening in het ziekenhuis. De afspraken die we daartoe onderling hebben gemaakt, zijn vastgelegd in de Verwerkingsovereenkomst St. Antonius Ziekenhuis - CMSB.

[19] Onderdeel van de procedure via de METC is vastlegging van de rechtvaardige verwerking van persoonsgegevens en toestemming van de patiënt.
[20] Studenten hebben een opleidingsovereenkomst maar zijn niet als werknemer in dienst van het ziekenhuis.

Het ziekenhuis neemt ook deel aan speciale, soms wat complexere, samenwerkingsverbanden. Het gaat dan bijvoorbeeld om regionale samenwerking met meerdere partijen of bijzondere projecten.

6.6.2. Santeon

De belangrijkste samenwerking in het kader van kwaliteitsverbetering is de samenwerking met zes andere ziekenhuizen verenigd in Santeon21. Dat doen we in het 'Samen beter' programma dat bestaat uit diverse thema's. Binnen Santeon worden persoonsgegevens voor twee hoofddoelen verwerkt, namelijk:

1. onderzoek ter verbetering van de kwaliteit van zorg, en
2. (medisch) wetenschappelijk onderzoek

De deelnemende ziekenhuizen leveren voor deze doelen pseudonieme of anonieme gegevens aan van hun eigen patiënten. Onderzoekers binnen Santeon kunnen de gegevens die zij ontvangen niet herleiden tot een individuele patiënt. De doorgifte van de gegevens is een verantwoordelijkheid van elk deelnemend ziekenhuis en vindt plaats op basis van ons beleid gegevensbescherming en informatiebeveiliging.

6.6.3. Overige samenwerkingen

Naast deze vaste samenwerkingspartners werkt het ziekenhuis ook met andere organisaties samen, bijvoorbeeld op projectbasis of in het kader van specifieke of tijdelijke afspraken. Ook dan kunnen persoonsgegevens worden gedeeld als dat noodzakelijk is voor de onderlinge dienstverlening.

6.7. Innovatie en Kunstmatige intelligentie (AI)

Naast wetenschappelijk onderzoek innoveert het St. Antonius Ziekenhuis ook op andere manieren, bijvoorbeeld met AI. Sinds enige tijd is er nadrukkelijk aandacht voor de toepassing van AI in onze samenleving. Ook binnen ons ziekenhuis maken we gebruik van AI. Dat doen we in feite al jaren, zij het dat de grootschalige en specifieke toepassingen die allemaal mogelijk zijn, nog maar vrij recent meer aandacht hebben gekregen. Inmiddels hebben we een AI-expertisecentrum opgericht waarin kennis, expertise en ervaringen van afdelingen met AI gebundeld worden.

We moeten als ziekenhuis waakzaam zijn dat gegevens van onze patiënten en medewerkers niet zomaar worden gebruikt en goed beschermd blijven. Dat betreft niet alleen de technische, maar ook de organisatorische bescherming. We moeten ons bij elke verwerking steeds afvragen of de specifieke doelen van de verwerking gerechtvaardigd zijn (geldige grondslag), of de gegevens die we willen verwerken ook echt nodig zijn (dataminimalisatie, subsidiariteit en proportionaliteit) en of we de betrokkenen wel voldoende hebben geïnformeerd over deze verwerkingen en toepassingen.
De Europese AI verordening stelt dat in de basis alle AI-systemen worden beschouwd als een duidelijke bedreiging voor de veiligheid, maar maakt wel onderscheid in risiconiveaus (van onacceptabel tot minimaal risico). Een voorbeeld van een hoog-risico AI-toepassing is robot ondersteunende chirurgie, maar ook AI-toepassing in wervingsprocedures.

[21] De andere zes ziekenhuizen zijn: CWZ (Nijmegen), OLVG (Amsterdam), Martini ziekenhuis (Groningen), Catharina Ziekenhuis (Eindhoven), Medisch Spectrum Twente (Enschede), Maasstad Ziekenhuis (Rotterdam).

Bijlagen

Bijlage 1 – Functie-eisen

Voor functies met een specifieke verantwoordelijkheid ten aanzien van gegevensbescherming en informatiebeveiliging gelden specifieke eisen ten aanzien van opleiding en certificering:

- CISO, PO, FG en I&I ISO, Afdelingshoofd Audit, Risk en Compliance en internal auditors (die onderdeel vormen van de afdeling AR&C) dienen te beschikken over tenminste 3 jaar relevante werkervaring en/of een relevant certificaat (waaronder CISSP, CISM, CISA). In overleg met HR kunnen deze eisen bij sollicitatieprocedures verhoogd worden.
- Assistent FG moet beschikken over relevante werkervaring en een training voor AVG en andere relevante wet- en regelgeving voor de gezondheidszorg.

Functievereisten voor overige rollen (bijvoorbeeld stagiaires) zijn vast te stellen door de leidinggevenden en/of PO/CISO in geval deze specifieke taken verrichten voor gegevensbescherming en informatiebeveiliging.

Bijlage 2 – Hoofdverantwoordelijkheden voor NEN 7510 en ISO 27001 hoofdstukken

Hoofdstuk	Hoofdverantwoordelijke(n)
A.5 Organisatorische beheersmaatregelen	RvB
A.6 Mensgerichte beheersmaatregelen	Manager HR
A.7 Fysieke beheersmaatregelen	Manager FZ
A.8 Technologische beheersmaatregelen	CIO

Bijlage 3 - Afwegingskader grondslag gerechtvaardigd belang

Voorwaarden	Uitleg
Voorwaarde 1: gerechtvaardigd belang	Beschrijf het **specifieke** belang van het ziekenhuis. Dat belang moet wel: Echt zijn. Dit houdt in dat het niet mag gaan om een mogelijk belang in de toekomst, waarvan u nog niet zeker bent. Concreet zijn. Dit houdt in dat u het belang duidelijk kunt verwoorden. Rechtstreeks zijn. Dit houdt in dat het gaat om een belang van uzelf, dus niet een algemeen belang van ‘de samenleving’ of iets dergelijks.
Voorwaarde 2 (a): noodzakelijkheid - **proportionaliteit**	Staat het doel van de verwerking in verhouding tot de inbreuk op de privacy van de betrokkenen?
Voorwaarde 2 (b): noodzakelijkheid - **subsidiariteit**	Kan het doel op een andere manier bereikt worden, dat minder ingrijpend is voor de betrokkenen?
Voorwaarde 3: afweging belangen	Maak een afweging tussen uw belangen en de belangen van de betrokkenen. Bij deze afweging kijkt u naar: - de gevolgen voor de betrokkenen; - hoe ernstig de inbreuk is op de privacy van de betrokkenen; - welke (aanvullende) maatregelen u heeft genomen om ongewenste gevolgen voor de betrokkenen te voorkomen of beperken; - of de betrokkenen de verwerking min of meer kunnen verwachten. Bijvoorbeeld als vervolg op een eerdere verwerking waarvoor zij toestemming hebben gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

NB: de belangenafweging betreft het belang van het ziekenhuis (voorwaarde 1) ten opzichte van het belang van de patiënt in relatie tot zijn rechten tot en de bescherming van zijn persoonsgegevens. Het gaat dus niet om het belang van een patiënt voor bijvoorbeeld goede zorgverlening of minder lang verblijf op de SEH.

Appendix 4 – English Summary for Suppliers

The St. Antonius Hospital has adopted a formal data protection and information security policy. This policy extends to suppliers, business partners and other collaborations. The most important compliance requirements concern the adherence to the GDPR and the Dutch NEN 7510 healthcare information security standard, which is based on the international ISO 27001 standard[22] and the NIS-2. Specific requirements are that supplier:

- Adheres to this policy and offers a protection level that meets or exceeds the requirements in this policy;
- Notifies the St. Antonius Hospital in case of information security incidents (including data leaks) in a timely manner;
- Notifies the St. Antonius Hospital of personnel changes at the supplier if those involved have direct access to systems at the St. Antonius Hospital. In case of normal termination or retirement this is done in advance, in case of involuntary termination this is done at the earliest opportunity.
- Regarding data protection, it is the policy of the St. Antonius Hospital to use the Model Data Processing Agreement from the Dutch the Association of Healthcare Providers (BoZ). Suppliers that process personal data in their role as processor are expected to sign this data protection agreement.[23]

[22] This standard is freely available from https://www.webtoolmanagementsystemen.nl/nl/NormDetail?standardId=cc28b925-3d18-4036-bd60-196465c9a05b&utm_campaign=webtool7510.

[23] Available from https://www.brancheorganisatieszorg.nl/nieuws_list/boz-modelverwerkersovereenkomst-vernieuwd/