ZIEKENHUIS
ST ANTONIUS

Beleid gegevensbescherming en informatiebeveiliging

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

Colofon
Datum: 31-10-2023
Informatie classificatie: publiek
Eindredactie: Corporate Information Security Officer

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.

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.

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

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. De reikwijdte van ons beleid wordt 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 door het opstellen van regels en richtlijnen waaraan ieder die in het ziekenhuis werkt zich dient te houden. De strenge eisen van de AVG gaan immers gepaard met hoge boetes in geval van overtreding hiervan. Bovendien hecht het St. Antonius Ziekenhuis er grote waarde aan dat patiënten, medewerkers en verwijzers erop kunnen vertrouwen dat gegevens bij ons in veilige handen zijn.

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.

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, dient een Data Protection Impact Assessment (DPIA)[1] uitgevoerd te worden. DPIAs behoren voorafgaand aan ingebruikneming plaats te vinden.
In geval van bestaande verwerkingen dient 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).

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.

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 matregelen 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.

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 komt een toezichthouder.

Onbekend is nog wel hoe deze richtlijn concreet vertaal zal worden naar Nederlandse wet- en regelgeving. Naar verwachting zal het St. Antonius Ziekenhuis eind 2024 moeten voldoen hieraan.

3. Het beleid

3.1. Missie, visie

Missie
Voor het St. Antonius Ziekenhuis is de volgende privacymissie geformuleerd: **"Het St. Antonius Ziekenhuis beschermt uw persoonsgegevens."**

Dit betekent onder meer dat we richting patiënten, maar ook richting medewerkers, aangeven dat:

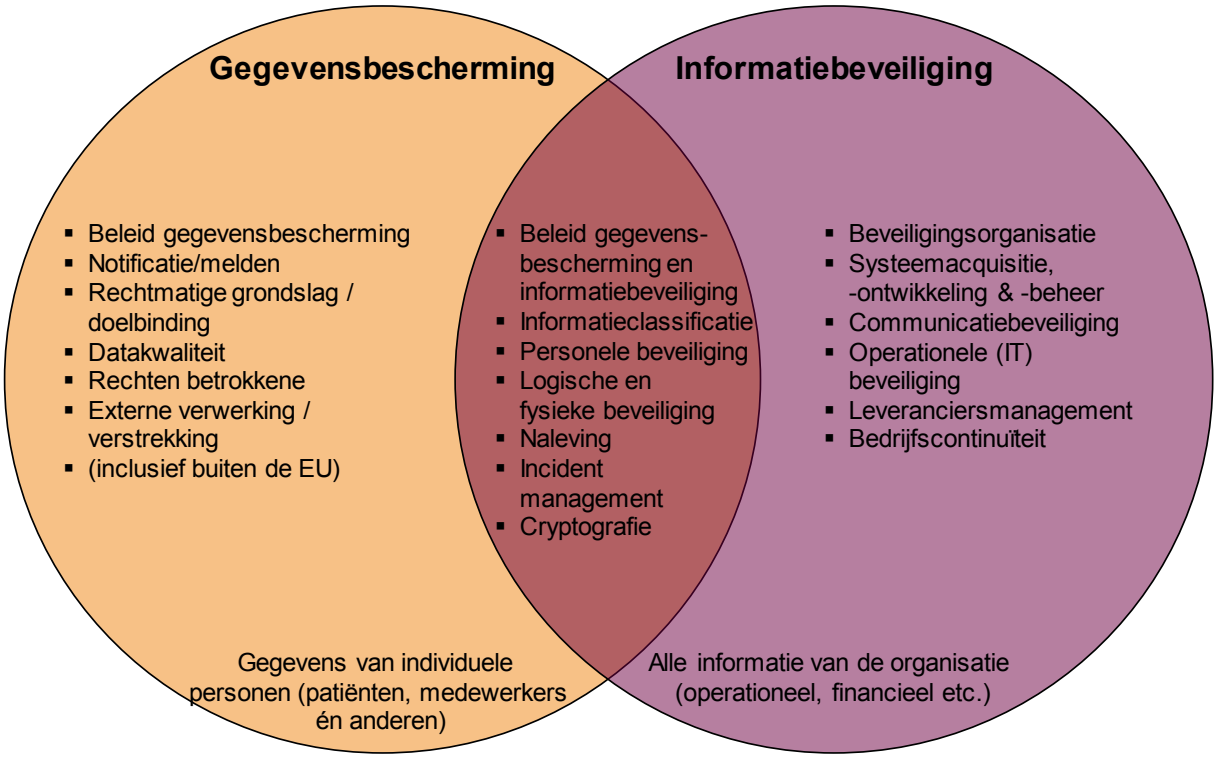
- We zorgvuldig omgaan met persoonlijke en medische gegevens;
- We zorgen dat onbevoegden geen toegang krijgen tot deze persoonsgegevens;
- We persoonsgegevens alleen gebruiken voor vastgestelde doeleinden; zodra deze gegevens niet meer nodig zijn voor de behandeling, zullen wij deze verwijderen en/of anoniem maken;
- Patiënten het recht hebben om wel/niet in te stemmen met het gebruik van gegevens voor medisch-wetenschappelijk onderzoek ten behoeve van het continu verbeteren van de zorgprocessen;
- Patiënten uitdrukkelijk toestemming moeten geven als deze (delen van) een patiëntdossier elektronisch raadpleegbaar wil maken voor andere zorgverleners; wij onze informatiesystemen, waarin deze gegevens zijn verankerd, beschermen tegen bedreigingen en onze beveiliging zo organiseren dat kwetsbaarheden worden verminderd, aanvallen worden verhinderd en schade wordt beperkt.

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.

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 PRIVACY 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 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

1. **De lijn is verantwoordelijk**
   Leidinggevenden dragen de primaire verantwoordelijkheid voor een zorgvuldige verwerking van informatie op hun afdeling/eenheid. Taken van de lijn omvatten de keuze de uitvoering, handhaving van maatregelen en risicoacceptatie. Onder de lijnverantwoordelijkheid valt ook 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.

2. **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.

3. **Geïnformeerde en risicogedreven besluitvorming**
   Bij wijzigingen, projecten en de aanschaf van informatiemiddelen is er een duidelijk beslismoment. Voorafgaand hieraan zijn verantwoordelijken geïnformeerd 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.

4. **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.

3.3.2. Gegevensbescherming

1. **Grondslag en doelbinding**
   Het St. Antonius Ziekenhuis zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

2. **Dataminimalisatie**
   Het St. Antonius Ziekenhuis verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Het St. Antonius Ziekenhuis streeft in samenwerking met de medische staf naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt en worden persoonsgegevens in zo min mogelijk systemen vastgelegd.

3. **Bewaartermijn**
   Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de zorgtaken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

4. **Integriteit en vertrouwelijkheid**
   Het St. Antonius Ziekenhuis gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen die schriftelijk geheimhouding hebben verklaard en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt het St. Antonius Ziekenhuis voor passende beveiliging van persoonsgegevens.

5. **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 controleert deze afspraken.

6. **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.

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

8. **Rechten**
   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.

9. **Register van verwerkingen**
   Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Het St. Antonius Ziekenhuis is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan zij de verwerkingsverantwoordelijke is. Dit register wordt opgezet en geactualiseerd door de Privacy Officer (PO), gedelegeerd aan de assistent FG.
   Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:
   - De naam en contactgegevens van de verwerkingsverantwoordelijke en (mogelijk) de gezamenlijke verwerkingsverantwoordelijke;
   - De doelen van de verwerking;
   - Een beschrijving van de soort persoonsgegevens en de daarbij horende betrokkenen;
   - Een beschrijving van de ontvangers van de persoonsgegevens;
   - Een beschrijving van het delen van persoonsgegevens aan een derde, land of internationale organisatie;
   - De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
   - Een algemene beschrijving van de beveiligingsmaatregelen.

   Het St. Antonius Ziekenhuis hanteert in beginsel een standaard verwerkersovereenkomst die door de Brancheorganisaties Zorg is ontwikkeld.

10. 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 in het St. Antonius Ziekenhuis, inclusief een format rapportage is beschikbaar.

11. Inzet van camera's

Binnen het ziekenhuis wordt gebruik gemaakt van cameratoezicht. Cameratoezicht gebruiken we onder andere voor 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. Het beleid is te vinden in het documentbeheersysteem op intranet.

12. Document retentiebeleid

In het beleid data bewaartermijnen (retentiebeleid), worden de afspraken vastgelegd voor het bewaren van bedrijfs- en persoonsgegevens op grond van ondernemingsbeleid en wettelijke verplichtingen. Met behulp van een consequent uitgevoerd document retentiebeleid verschaft het St. Antonius Ziekenhuis duidelijkheid over het bewaren en vernietigen van documenten. In een document retentie beleid wordt per soort document bepaald hoelang het moet worden bewaard, in welke vorm, op welke (fysieke of digitale) locatie en wie daarvoor verantwoordelijk is.

13. 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. Incidenten worden vanwege de efficiency bij voorkeur gemeld aan de I&I Helpdesk. Indien de melder daar de voorkeur aan geeft kan dit ook vertrouwelijk bij de FG.

Van elk incident en de afhandeling daarvan wordt een registratie bijgehouden. Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen persoonlijke consequenties heeft. Een melder dient 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.

14. 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.

15. **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.

16. **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

1. **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 IT systemen zoveel mogelijk worden verholpen ongeacht de ernst ervan.

2. **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.

3. **De afdeling I&I is de "preferred partner" voor 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 die buiten deze governance om werken, zullen zelfstandig moeten kunnen aantonen dat zij informatiebeveiliging borgen.

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-check-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 door de bestuursadviescommissie gegevensbescherming en informatiebeveiliging en de adviesgremia.

Indien beleidswijzigingen aanzienlijke impact hebben op de werkwijze van de organisatie vindt consultatie hierover plaats met de leidinggevenden van de belanghebbenden, de bestuursadviescommissie gegevensbescherming en informatiebeveiliging en/of de adviesgremia. Organisatieonderdelen zijn bevoegd om hun eigen beleidsdocumenten op te stellen, mits deze:

- Niet strijdig zijn met het bestaande beleid of het vervangen;
- 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.

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 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.

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 ISMS 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.

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, wij vragen 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 (bijvoorbeeld de informatiemanagers);
- 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.[2]

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 continuïteit van onze bedrijfsvoering te borgen.

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.

De evaluatie van beveiligingsincidenten wordt eveneens benut voor het continu verbeteren van informatiebeveiliging. 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 helpdesk Buiten kantoortijden per telefoon (alleen bij grote incidenten)
Zorggerelateerde incidenten	Veilig Incident Melden / Melden incident medewerker: Vanaf werkplek: Start > Incidentmelding VIM en MIM

[2] 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[3].

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.

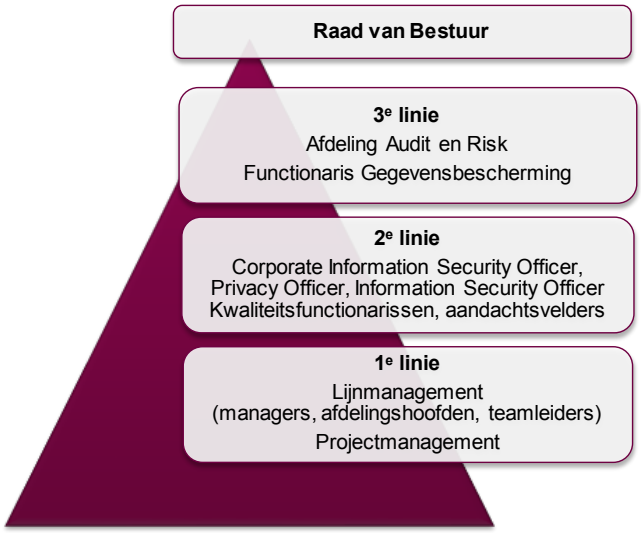
Aandachtsvelders
Op operationeel niveau kan per eenheid een ISO en/of aandachtsvelder vrijgemaakt worden om enkele uren per week specifiek te werken aan instandhouding en verbetering van gegevensbescherming en informatiebeveiliging, bijvoorbeeld voor het beantwoorden van vragen, het wijzen op (mogelijke) 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 of 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

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

Persoonsgegevens toezicht op de uitvoering van de AVG en rapporteert eveneens direct aan het bestuur.



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 dient als managementforum, conform de NEN 7510 en ISO 27001. De commissie 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:
  a. Aangelegenheden die in relatie staan tot gegevensbescherming van patiënten, medewerkers en hun onderlinge relatie en die in relatie staan met de stichting;
  b. Aangelegenheden die in relatie staan tot informatiebeveiliging van de stichting;
  c. Het goedkeuren van relevante beleidsdocumenten;
  d. 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.[4]
- 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 geeft invulling aan de eis uit de NEN 7510 en ISO 27001 voor het instellen van een informatiebeveiligingsmanagementforum[5].
- De commissie heeft geen normstellende bevoegdheden bij het bepalen van de inrichting van het elektronische patiëntendossier.

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.

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.

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

[5] NEN 7510-1+A1:2020 A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging:
Organisaties moeten: (…) over een informatiebeveiligingsmanagementforum (IBMF) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B.3 en B.4 van bijlage B (NEN 7510-2). (…)
Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. (…)

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[6];
- 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:

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

- Het volgen van de vereiste projectmethodiek inclusief het uitvoeren van BIA's (business impact analyses), DPIA's (data protection impact assessments) en (prospectieve) risicoanalyses;
- 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.

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.

Ondernemingsraad
De ondernemingsraad ziet toe op de uitvoer van het informatiebeveiligingsbeleid en relevante wet- en regelgeving vanuit het oogpunt van de werknemers.

5.3.3. Individuele rollen en functionarissen

Chief Medical Information Officer (CMIO)
De CMIO bemoeit zich 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 bemoeit zich 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.

Chief Medical Data Officer (CMDO)
De CMDO richt zich specifiek op het genereren van op data gebaseerde informatie ten behoeve van het continu verbeteren van uitkomsten en het ontwikkelen en stimuleren van clinical data science: een specifiek deelgebied waar de ontwikkelingen nog in de kinderschoenen staan.

Manager Inkoop
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. Het Inkoopbeleid wordt door de Manager Inkoop vastgelegd.

Manager HR
De manager HR 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 HR borgt dat arbeidsovereenkomsten en gastovereenkomsten eisen tot geheimhouding en naleving van de gedragcode (waaronder het beleid gegevensbescherming informatiebeveiliging) bevatten.

Manager Marketing en Communicatie
De manager Marketing en Communicatie (M&C) zorgt 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 afdeling M&C 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 bedrijfsvoering en medisch manager Klinische Fysica & Instrumentatie
De manager bedrijfsvoering en medisch manager Klinische Fysica & Instrumentatie 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 Faciliteiten & Vastgoed
De manager Faciliteiten & Vastgoed 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.

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.

5.3.4. Gegevensbescherming en informatiebeveiliging functionarissen

Corporate Information Security Officer (CISO)
De CISO heeft een rol op strategisch niveau. Hij rapporteert aan de manager ARC, 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 ARC 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 root cause analyses;
- Onderhoudt contacten met speciale belangengroepen;
- Richt het control framework programma in;
- Vervangt de FG bij afwezigheid.

Functionaris Gegevensbescherming (FG)
De FG ziet toe op de implementatie van de Algemene Verordening Gegevensbescherming (AVG) 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. De FG vervangt de CISO bij afwezigheid.[7]

Privacy Officer (PO)
De privacy officer[8]:
- 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 privacy vraagstukken;
- 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.

[7] 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 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.
[8] De Privacy officer is een rol die bij één of meerdere personen kan worden belegd.

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 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 informatiebeveiligingsbeleid en zorgen voor bewustwording bij collega's;
- Mede-implementeren en borgen van het informatiebeveiligingsbeleid op de afdeling;
- Beantwoorden van vragen van medewerkers van de afdeling over gegevensbescherming en informatiebeveiliging;
- (Helpen bij) het melden van informatiebeveiligingsincidenten;
- Assisteren bij acties die voortvloeien uit informatiebeveiligingsincidenten;
- 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.

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.

5.3.5. 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.

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 privacy, security 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 17) 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.

5.3.6. 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 dient 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.

Bijlagen

Bijlage 1 – Privacy gedragsregels en reglement

Gedragsregels

Gedragsregels geven aan hoe de organisatie wil dat medewerkers reageren op privacyvraagstukken en eventuele afwijkingen op het beleid. Bij het opstellen van de privacy gedragsregels zijn de zogenaamde European Fair Information Principles (FIP) gehanteerd.

Voor het St. Antonius Ziekenhuis betekent dit het volgende:

1. Alleen persoonsgegevens die relevant zijn voor een goede behandeling van de patiënt - en om te voldoen aan wettelijke eisen- leggen we vast, mits op rechtmatige wijze en met specifieke toestemming van de betrokkene verkregen. De patiënt informeren we hierover.
2. Persoonsgegevens verwerken we alleen voor de identificatie van de patiënt, voor een goede en zorgvuldige behandeling, voor een zorgvuldige overdracht binnen de zorgketen en voor de financiële afwikkeling van de facturatie. Bij elk patiëntbezoek controleren we of de vastgelegde patiëntgegevens nog actueel zijn. Voor gebruik van data voor medisch/wetenschappelijk onderzoek kan de patiënt expliciet aangeven of hij/zij daar wel/niet aan wil deelnemen. Ook dient de patiënt expliciet aan te geven of hij/zij toestemming geeft voor beschikbaar stellen van zijn gegevens aan zorgverleners buiten het St. Antonius Ziekenhuis.
3. De patiëntgegevens gebruiken we alleen voor de onder punt 2 genoemde doeleinden en voor het voldoen aan wettelijke verplichtingen zoals landelijke kwaliteitsregistraties.
4. Op de publieke website van het St. Antonius Ziekenhuis en op intranet publiceren we het privacyverklaring en de gedragsregels met vermelding van de contactgegevens van de verwerkingsverantwoordelijke en van de functionaris gegevensbescherming.
5. De rechten van betrokkenen omvatten het recht op informatie omtrent de persoonsgegevens, recht op inzage, rectificatie en klachten, recht op actualisatie, (deel) weigering van verwerking, vergetelheid en dataportabiliteit. Het St. Antonius Ziekenhuis zal deze rechten bekend maken aan betrokkenen via informatie op de website. Een verzoek van een betrokkene zal het St. Antonius Ziekenhuis binnen 4 weken na ontvangst afhandelen. Een verzoek tot volledige verwijdering van alle gegevens duurt maximaal 3 maanden.
6. Indien een patiënt of betrokkene klachten heeft over de naleving van zijn rechten, bestaat de mogelijkheid om een klacht in te dienen bij de functionaris gegevensbescherming.
7. Het St. Antonius Ziekenhuis past geen geautomatiseerde profilering toe op basis van persoonsgegevens.

Privacyreglement

Artikel 1 Begripsbepalingen

1.1 *Persoonsgegeven*: Alle gegevens die gaan over personen en waaraan je een persoon als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of de gezondheid.
1.2 *Verwerking:* Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen
1.3 *Betrokkene*: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
1.4 *Verwerkingsverantwoordelijke:* Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
1.5 Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
1.6 *Gebruiker*: degene, die onder verantwoordelijkheid van de verantwoordelijke ten behoeve van de taakuitoefening, toegang heeft tot de verwerking en bevoegd is gegevens in te voeren en/of te wijzigen.

1.8 *Autoriteit Persoonsgegevens*: De AP heeft tot taak toe te zien op de verwerking van persoonsgegevens.

Artikel 2 Reikwijdte van het reglement
2.1 Dit reglement is van toepassing binnen het Sint Antonius Ziekenhuis en heeft betrekking op alle gegevensverwerkingen van patiënten, medewerkers en overige personen.
2.2 Dit reglement geldt voor alle verwerkingen van persoonsgegevens, geautomatiseerd of niet geautomatiseerd, uitgevoerd in opdracht van het Sint Antonius Ziekenhuis door medewerkers van het ziekenhuis en door in het Sint Antonius Ziekenhuis toegelaten beroepsbeoefenaren.

Artikel 3 Doel
3.1 Doel van dit reglement is een praktische uitwerking te geven aan de bepalingen van de Algemene Verordening Gegevensbescherming (verder AVG) en –voor zover van toepassing- de Wet geneeskundige behandelingsovereenkomst (Wgbo).

Artikel 4 Voorwaarden voor rechtmatige verwerking
4.1 Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (grondslagen) verzameld.
4.2 Persoonsgegevens worden verwerkt op een wijze die verenigbaar is met de doeleinden beschreven in het in artikel 2.1 genoemde overzicht van verwerkingen.
4.3 Verwerking van persoonsgegevens dient nauwkeurig, compleet en actueel te zijn en niet meer te omvatten dan voor het doel van de gegevensverwerking nodig is (dataminimalisatie).

Artikel 5 Grondslagen voor verwerking van persoonsgegevens
Persoonsgegevens mogen slechts worden verwerkt indien aan één van de volgende wettelijke grondslagen is voldaan:
- Het is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor handelingen die op verzoek van de betrokkene worden verricht.
- Het is noodzakelijk om aan een wettelijke verplichting te voldoen.
- Het is noodzakelijk ter bestrijding van ernstig gevaar voor de gezondheid van betrokkene.
- Het is noodzakelijk voor de vervulling van een publiekrechtelijke taak.
- Het is noodzakelijk met het oog op het belang van de verantwoordelijke.
- De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend.

Artikel 6 Beheer van de verwerkingen van persoonsgegevens
6.1 De verantwoordelijke houdt een register bij van in het Sint Antonius ziekenhuis gehanteerde verwerkingen waarbij persoonsgegevens zijn betrokken (door de functionaris gegevensbescherming).
6.2 De verantwoordelijke wijst een eigenaar/verantwoordelijke aan voor elk van de in het ziekenhuis gebruikte verwerkingen. Deze is verantwoordelijk voor de verwerking van persoonsgegevens conform de AVG.
6.3 Een nieuwe verwerking van persoonsgegevens dient door de eigenaar/verantwoordelijke te worden aangemeld bij de functionaris gegevensbescherming.

Artikel 7 Kennisgeving
De verantwoordelijke deelt vóór het moment van verkrijging van de persoonsgegevens de betrokkene zijn rechten mede en geeft aan met welke doeleinden de persoonsgegevens worden verwerkt. Indien de gegevens van derden zijn verkregen, dan wordt de bron vermeld. De betrokkene hoeft niet te worden geïnformeerd indien de verantwoordelijke er redelijkerwijze vanuit mag gaan dat deze bekend is met de verwerkingen van persoonsgegevens en de betreffende doeleinden.

Artikel 8 Vertegenwoordiging wat betreft medische persoonsgegevens
De verplichtingen uit dit reglement worden nagekomen tegenover de betrokkene of zijn vertegenwoordiger.
1. Indien de betrokkene jonger is dan twaalf jaar treden de ouders die het ouderlijk gezag uitoefenen dan wel de voogd op in plaats van de betrokkene.
2. Hetzelfde geldt voor de betrokkene die de leeftijd van twaalf jaar heeft bereikt en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake.

3. Indien de betrokkene in de leeftijdscategorie van twaalf tot zestien valt en in staat is tot een redelijke waardering van zijn belangen, treden naast de betrokkene zelf diens ouders op.
4. Indien de betrokkene zestien of zeventien jaar is kan deze zonder toestemming van degene die gezag over hem uitvoert zelf zijn rechten geldend maken.
5. Indien de betrokkene ouder is dan achttien jaar en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake, dan treedt, in volgorde zoals hier weergegeven, als vertegenwoordiger voor hem op:
- de curator of mentor indien de betrokkene onder curatele staat of ten behoeve van hem het mentorschap is ingesteld;
- de persoonlijke gemachtigde indien de betrokkene deze schriftelijk heeft gemachtigd, tenzij deze persoon niet optreedt;
- de echtgenoot of andere levensgezel van de betrokkene, tenzij deze persoon dat niet wenst of ontbreekt;
- een kind, broer of zus van de betrokkene, tenzij deze persoon dat niet wenst.

6. Echter ook indien de betrokkene de leeftijd van zestien jaar heeft bereikt en wel in staat is tot een redelijke waardering van zijn belangen, heeft hij de mogelijkheid een andere persoon schriftelijk te machtigen en in diens plaats als vertegenwoordiger op te treden.
7. De toestemming kan door de betrokkene of zijn vertegenwoordiger te allen tijde worden ingetrokken.

Artikel 9 Verstrekking van gegevens aan derden
9.1 Tenzij dit geschiedt ter uitvoering van een wettelijke bepaling, een overeenkomst, ter vervulling van een publiekrechtelijke taak of het een geval betreft zoals genoemd in de volgende leden van dit artikel is voor de verstrekking van persoonsgegevens aan derden de gerichte toestemming van de betrokkene vereist.
9.2 Binnen de instelling kunnen zonder toestemming van de betrokkene persoonsgegevens worden verstrekt, voor zover dit voor hun taakuitoefening noodzakelijk is, aan:
- Degenen die betrokken zijn bij de actuele zorg- of hulpverlening aan betrokkenen.
- Degenen die betrokken zijn bij de financiële en administratieve afhandeling van de zorg- of hulpverlening van betrokkenen.

9.3 Persoonsgegevens worden niet overgebracht naar landen buiten de Europese Unie tenzij dat land een adequaat niveau van de bescherming van rechten en vrijheden van personen kan garanderen met betrekking tot het verwerken van persoonsgegevens.
9.4 Persoonsgegevens kunnen alleen dan zonder toestemming van de betrokkene ten behoeve van wetenschappelijk onderzoek en statistiek worden verstrekt indien aan één van de volgende voorwaarden is voldaan:
a. Het vragen van gerichte toestemming in redelijkheid niet mogelijk is en voorzien is in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.
b. Het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener er zorg voor heeft gedragen dat de gegevens in zodanige anonieme vorm worden verstrekt dat herleiding tot individuele personen redelijkerwijs wordt voorkomen.

Voorts is dit slechts mogelijk indien:
- het onderzoek een algemeen belang dient;
- het onderzoek niet zonder desbetreffende gegevens kan worden uitgevoerd;
- de betrokken patiënt ingestemd heeft met het gebruik van zijn gegevens.

9.5 Van het lichaam afgescheiden stoffen en delen (zoals weefsel of huid) kunnen worden gebruikt voor medisch statistisch of ander wetenschappelijk onderzoek als aan de volgende drie voorwaarden is voldaan:
- gewaarborgd moet zijn dat het materiaal en de gegevens die daaruit te verkrijgen zijn niet tot de persoon herleidbaar is;
- de patiënt van wie het lichaamsmateriaal afkomstig is, heeft toegestemd met het mogelijke gebruik;
- het onderzoek moet met de vereiste zorgvuldigheid worden verricht.

Artikel 10 Toegang tot persoonsgegevens
10.1 De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies, vernietiging, en onrechtmatige toegang, wijziging, verwerking en openbaring. Deze maatregelen garanderen rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Bescherming van digitale persoonsgegevens wordt geregeld in het informatiebeveiligingsbeleid.
10.2 Gebruikers mogen toegang hebben tot persoonsgegevens voor zover dit noodzakelijk is voor het uitoefenen van hun functie.

Artikel 11 Inzage en afschrift van persoonsgegevens
11.1 De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende geregistreerde gegevens.
11.2 De gevraagde inzage en/of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen één maand na ontvangst van het verzoek worden gehonoreerd.
11.3 Verzoeken tot inzage of afschrift worden schriftelijk ingediend bij de verantwoordelijke. Dit verzoek wordt ondertekend door de betrokkene.
11.4 De verantwoordelijke bepaalt wie belast wordt met de uitvoering van de inzage of het verstrekken van een afschrift.
11.5 De verantwoordelijke kan weigeren aan een verzoek te voldoen, indien en voor zover dit noodzakelijk is in verband met:
a. De opsporing en vervolging van strafbare feiten;
b. Gewichtige belangen van anderen dan de verzoeker, de verantwoordelijke daaronder begrepen.
11.6 Voor de verstrekking van extra afschriften of bij herhaaldelijke verzoeken kan een vergoeding in rekening worden gebracht.

Artikel 12 Aanvulling, correctie, beperking gebruik of vernietiging van opgenomen persoonsgegevens
12.1 Desgevraagd worden de in een verwerking van persoonsgegevens opgenomen inlichtingen aangevuld met een door de betrokkene afgegeven verklaring met betrekking tot deze informatie.
12.2 De betrokkene kan de verantwoordelijke verzoeken om correctie van de op hem betrekking hebbende gegevens. De verantwoordelijke is alleen verplicht te corrigeren indien de gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn of op andere wijze in strijd zijn met een voorschrift van de AVG of een andere wet zijn verwerkt. De verantwoordelijke deelt binnen acht weken na ontvangst van het verzoek de betrokkene zijn beslissing mee. Een weigering tot correctie over te gaan wordt met redenen omkleed.
12.3 De betrokkene kan zijn verleende toestemming voor gebruik van zijn gegevens voor medisch/-wetenschappelijk onderzoek te allen tijde intrekken of opnieuw verstrekken.
12.4 De betrokkene kan de verantwoordelijke schriftelijk verzoeken om vernietiging van tot zijn persoon herleidbare gegevens. Er is een procedure die gevolgd wordt indien een verzoek tot vernietiging van het medische en verpleegkundig dossier de verantwoordelijke bereikt. De gegevens zullen niet worden verwijderd, indien deze nog nodig zijn vanuit andere wettelijke voorschriften.

Artikel 13 Bewaartermijnen
13.1 Met inachtneming van de geldende wettelijke voorschriften stelt de verantwoordelijke vast hoe lang de in de verwerking opgenomen persoonsgegevens bewaard blijven.
13.2 De bewaartermijn van het medische en verpleegkundig patiëntendossier is tenminste 20 jaar, te rekenen vanaf de laatste behandeling door het betreffende specialisme in het Sint Antonius ziekenhuis, of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.
13.3 De bewaartermijn van personeelsgegevens is maximaal tot twee jaar na beëindiging van het dienstverband of het verrichten van werkzaamheden, tenzij deze gegevens in verband met wettelijke verplichtingen langer bewaard moeten blijven.
13.4 De bewaartermijn van afschriften van bepaalde documenten op grond van de WvGGZ, zoals rechterlijke beslissingen en geneeskundige verklaringen, genoemd in artikel 56 lid 3 Wet WvGGZ, is vijf jaar, te rekenen vanaf het tijdstip waarop de behandeling in het kader van de WvGGZ op de plaatsing in het ziekenhuis is beëindigd.
13.5 Indien de bewaartermijn is verstreken worden de betreffende persoonsgegevens zo mogelijk verwijderd en vernietigd. Vernietiging blijft echter achterwege wanneer redelijkerwijs aannemelijk is

dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, of indien daarover tussen de betrokkene en de beroepsbeoefenaar overeenstemming bestaat.
13.6 Indien de betreffende gegevens zodanig zijn bewerkt dat herleiding tot individuele personen redelijkerwijs onmogelijk is kunnen zij in geanonimiseerde vorm bewaard blijven.

Artikel 14 Klachten
14.1 Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of hij andere redenen heeft om aan te nemen dat de AVG niet correct wordt uitgevoerd in het Sint Antonius ziekenhuis dient hij zich te wenden tot een door de verantwoordelijke hiervoor aangewezen persoon of de functionaris gegevensbescherming.
14.2 Indien dit voor de betrokkene niet leidt tot een acceptabel resultaat heeft hij de volgende mogelijkheden:
- De binnen de instelling functionerende regeling voor onafhankelijke klachtenbehandeling of, in geval van personeelsgegevens, de Raad van Bestuur.
- De AP verzoeken een onderzoek in te stellen of de wijze van gegevensverwerking door de verantwoordelijke in overeenstemming is met de AVG.

Bijlage 2 – 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 3 – Hoofdverantwoordelijkheden voor NEN 7510 en ISO 27001 hoofdstukken

Hoofdstuk	Hoofdverantwoordelijke(n)
A.5 Informatiebeveiligingsbeleid	RvB
A.6 Organiseren van informatiebeveiliging	RvB
A.7 Veilig personeel	Manager HR
A.8 Beheer van bedrijfsmiddelen	CIO
A.9 Toegangsbeveiliging	CIO
A.10 Cryptografie	CIO
A.11 Fysieke beveiliging en beveiliging van de omgeving	Manager F&V
A.12 Beveiliging bedrijfsvoering	CIO
A.13 Communicatiebeveiliging	CIO
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen	CIO
A.15 Leveranciersrelaties	Alle afdelingen
A.16 Beheer van informatiebeveiligingsincidenten	CIO
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	RvB
A.18 Naleving	RvB

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.[9] 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.[10]

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

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