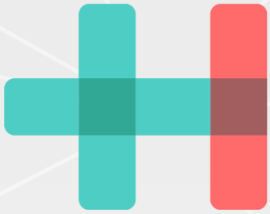


HealthConnected

Privacy- en informatiebeveiligingsbeleid

Versie 3.1 Auteur Dieter Vorderhake Datum 25-1-2023
Classificatie OPENBAAR

1. Inleiding

Dit document beschrijft het beleid van HealthConnected met betrekking tot privacy en informatiebeveiliging. Informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van HealthConnected. Zowel op papier als geautomatiseerd is HealthConnected bij het dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. De organisatie en de informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Het proces van privacy en informatiebeveiliging begint met het definiëren van een beleid op dit punt. Dit beleid is vastgelegd in het onderhavige document.

1.1 Een definitie van privacy en van informatiebeveiliging

Privacy wordt als volgt gedefinieerd:
Het betekent dat iemand dingen kan doen zonder dat de buitenwereld daar weet van heeft, inbreuk op maakt, of invloed op heeft. De afscherming van beïnvloeding wordt ook omschreven als het recht om met rust gelaten te worden. Het is een universeel mensenrecht, een fundamentele vrijheid en een grondrecht.

Privacy gaat om de afscherming van persoonsgegevens, het eigen lichaam, de woning of leefruimte, familie- en gezinsleven. Privacy omvat ook het recht vertrouwelijk te communiceren, zoals via brief, telefoon, e-mail.

Informatiebeveiliging wordt als volgt gedefinieerd:
Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen.

Opgemerkt wordt dat informatiebeveiliging een *samenhangend stelsel van maatregelen* omvat. Voor zowel het beschermen van de privacy als informatie betekent dit dat de verschillende maatregelen die tezamen de privacy- en informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Het stelsel van beveiligingsmaatregelen heeft tot doel een blijvend niveau van beveiliging te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn gehandhaafd blijft. Privacy – en informatiebeveiliging is gericht op het realiseren van een optimaal niveau van beveiliging. Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

1.2 Doelstelling privacy- en informatiebeveiligingsbeleid

Het privacy- en informatiebeveiligingsbeleid legt de doelstellingen en uitgangspunten met betrekking tot privacy en beveiliging van informatie binnen HealthConnected vast. Hiermee vormt het beleid de leidraad voor alle medewerkers binnen HealthConnected. HealthConnected heeft privacy en informatiebeveiliging hoog in het vaandel staan, omdat zij:

- privacy van personen wil waarborgen;
- persoonsgegevens wil beveiligen;
- het bewustzijnsniveau m.b.t. privacy en informatiebeveiliging onder de medewerkers wil vergroten;
- wil voldoen aan wet- en regelgeving;
- wil aantonen door middel van certificering dat zij betrouwbaar omgaat met privacy en informatie en dat zij hierdoor een betrouwbare partner is (realiseren van klantenbinding).

1.3 Doelstelling privacy en informatiebeveiliging

Doelstelling privacy:
Privacy is een grondrecht. En een voorwaarde om vrij te zijn in wie je bent en wat je doet. Het doel van privacy in dit beleid is:

- dat personen regie (zeggenschap) houden over hun gegevens;
- dat personen niet continu gevolgd worden;
- dat medische gegevens veilig zijn;
- dat personen iets kunnen doen tegen een automatisch genomen besluit.

HealthConnected is een verwerker van PII (Personal Identifiable Information) en zal bij de ontwikkeling van haar software en bij de verwerking van persoonsgegevens met behulp van haar software zorgdragen dat bovengenoemde privacy doelstellingen kunnen worden uitgevoerd. Dit vertaalt zich in:

- Het kunnen uitoefenen van rechten die personen hebben onder de AVG (recht op informatie –wat is de verwerking-, inzage, rectificatie, vergetelheid en dataportabiliteit);
- Het proactief beperken van het delen en loggen van informatie naar wat strikt noodzakelijk is;
- Het beschermen van persoonsgegevens met behulp van technische en organisatorische maatregelen;
- Het kunnen terugdraaien of corrigeren van automatische genomen besluiten;

Om deze doelstellingen te halen zijn er processen ingericht. Deze processen worden periodiek gecontroleerd.

Doelstelling informatiebeveiliging:
Zoals in de definitie van informatiebeveiliging is verwoord, is het doel van informatiebeveiliging om een optimaal niveau te realiseren van:

- **Beschikbaarheid:** de informatie moet op de gewenste momenten beschikbaar zijn;
- **Integriteit:** de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- **Vertrouwelijkheid:** de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Om te kunnen bepalen wat het niveau is van beschikbaarheid, integriteit en vertrouwelijkheid en of het aan de eisen voldoet, zijn er periodieke controles ingericht op maandelijkse, kwartaal en halfjaarlijkse basis. Deze controles bestaan uit administratieve en technische controles en zijn direct gerelateerd aan de beschikbaarheid, integriteit en vertrouwelijkheid. De acceptatiecriteria zijn:

- 90% - 100% acceptabel
- 70% - 90% acceptabel, wel melden als verbeterpunt
- 0% - 70% onacceptabel, direct melden bij directie

Het percentage van de controles worden bepaald op basis van tellingen (goed/fout) tijdens de controles. Deze kunnen bestaan uit tellingen van servers, laptops/computers, medewerkers, accounts & steekproeven van procedures. Daarnaast zijn er nog controles op basis van (interne en externe) audits, PEN testen en restore testen waarbij de uitkomst in zijn geheel goed of fout is.

De uitkomst van de periodieke controles wordt gerapporteerd in de kwartaalrapportage en bij afwijkingen behandeld in het directieoverleg (zie §4.5).

1.4 Werkingsgebied

Het privacy- en informatiebeveiligingsbeleid is van toepassing op:

Ontwerpen, ontwikkelen en functioneel beheer van HealthConnected software voor elektronische patiëntdossiers in de eerstelijnszorgverlening.

HealthConnected hanteert als uitgangspunt dat zij verantwoordelijk is voor de correcte verwerking van alle gegevens die door klanten met behulp van HealthConnected software worden vastgelegd. HealthConnected is daarbij verantwoordelijk voor het treffen van passende technische en organisatorische maatregelen bij het ontwikkelen, beheren, hosten en ondersteunen van deze HealthConnected software.

HealthConnected is nadrukkelijk niet verantwoordelijk voor de apparatuur waarop onze producten worden gebruikt, de juistheid van de uit andere bronnen verkregen of handmatig ingevoerde data en de werking van aan HealthConnected software gekoppelde applicaties.

HealthConnected faciliteert gebruikers van HealthConnected software bij het voldoen aan de voor hen van toepassing zijnde wet- en regelgeving. HealthConnected is niet verantwoordelijk voor de wijze waarop gebruikers van HealthConnected software ook daadwerkelijk gebruik maken van deze mogelijkheden.

Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie. Een uitleg over de context waarbinnen HealthConnected opereert is te vinden in het managementsysteem (ISMS / PIMS).

1.5 Verantwoordelijkheid privacy- en informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het privacy- en informatiebeveiligingsbeleid.

De CISO is verantwoordelijk voor het onderhoud van het privacy- en informatiebeveiligingsbeleid.

1.6 Ondersteunende documentatie

Dit privacy- en informatiebeveiligingsbeleid is binnen HealthConnected verder uitgewerkt in o.a. de volgende documenten:

- Handboek privacy en informatiebeveiliging;
- Onderliggend beleid;
- Werkinstructies;
- Managementsysteem (ISMS / PIMS).

Een overzicht van alle documenten is te vinden in het managementsysteem (ISMS / PIMS). De documenten zijn opgeslagen op de gedeelde schijf binnen de beveiligde kantooromgeving.

1.7 Middelen

HealthConnected gebruikt de volgende middelen voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem (ISMS / PIMS) voor privacy en informatiebeveiliging:

- Microsoft Office;

    - Word: opstellen beleidstukken, procesbeschrijvingen, werkinstructies en overige documenten;
    - Excel: inrichten, registreren en onderhouden van het managementsysteem (ISMS / PIMS) en risicoanalyses;
- Adobe Acrobat; (intern) publiceren van beleidstukken, procesbeschrijvingen, werkinstructies en overige documenten;
- Gedeelde schijf (binnen de beveiligde kantooromgeving): opslag voor alle documenten binnen HealthConnected.

1.8 Inhoud privacy- en informatiebeveiligingsbeleid

In hoofdstuk 2 zijn de uitgangspunten vastgelegd die worden gehanteerd bij de toepassing van privacy en informatiebeveiliging binnen HealthConnected. In hoofdstuk 3 wordt aandacht besteed aan het beleidsproces voor privacy en informatiebeveiliging. Hoofdstuk 4 beschrijft de organisatie van privacy en informatiebeveiliging.

2. Uitgangspunten privacy en informatiebeveiliging

Bij de toepassing van privacy en informatiebeveiliging binnen HealthConnected worden de volgende uitgangspunten gehanteerd:

- HealthConnected voldoet aantoonbaar aan de ISO 27001 en NEN 7510 normen.
- HealthConnected voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
    - Algemene Verordening Gegevensbescherming (AVG)
    - Electronic Identities And Trust Services (eIDAS)
    - Besluit elektronische gegevensverwerking door zorgaanbieders
    - Wet elektronische gegevensuitwisseling in de zorg (Wegiz)
    - Wet Computer Criminaliteit (WCC)
    - Wet Geneeskundige Behandelingsovereenkomst (WGBO)
    - Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG)
- Beveiliging van privacy en informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle onderdelen van HealthConnected hebben hiertoe verantwoordelijkheden voor privacy en informatiebeveiliging toegewezen en vastgelegd. De in hoofdstuk 4 beschreven organisatie van privacy en informatiebeveiliging vormt hierbij de leidraad.
- Wanneer (onderdelen van) HealthConnected samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan privacy en informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
- De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van HealthConnected zijn volgens een gestructureerde methode geclassificeerd.
- Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
- HealthConnected voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren.

- HealthConnected beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
- Bij overtreding van de regelgeving voor privacy en informatiebeveiliging en/of relevante wettelijke bepalingen kan de directie een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in het handboek privacy en informatiebeveiliging.
- Alle onderdelen van HealthConnected hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
- Alle onderdelen van HealthConnected hebben maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, etc.) vormen hiervan een belangrijk onderdeel.
- Alle onderdelen van HealthConnected hebben maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
- Bij de ontwikkeling en aanschaf van informatiesystemen wordt in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan privacy en informatiebeveiliging.
- Alle onderdelen van HealthConnected hebben adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
- Als onderdeel van het beleidsproces voor privacy en informatiebeveiliging wordt binnen HealthConnected door interne en externe partijen toegezien op de naleving van het privacy- en informatiebeveiligingsbeleid.
- Alle onderdelen van HealthConnected beschikken over middelen voor het melden en afhandelen van privacy- en informatiebeveiligingsincidenten. De evaluatie van de afhandeling van privacy- en informatiebeveiligingsincidenten wordt benut voor de verbetering van privacy en informatiebeveiliging.

2.1 Cyber resilience

Het is van belang de negatieve gevolgen van uitval van primaire bedrijfsprocessen (en onderliggende technische kwetsbaarheden) zoveel mogelijk te beperken. Hiertoe zijn continuïteitsvoorzieningen getroffen. Per bedrijfsproces en technische kwetsbaarheid wordt bepaald en vastgelegd welke voorzieningen getroffen zijn om de continuïteit van de primaire bedrijfsprocessen zoveel mogelijk te waarborgen.

Prepare/Identify

In deze fase worden alle bedrijfsprocessen en technische kwetsbaarheden in kaart gebracht en vastgelegd in het cyber resilience overzicht.

Protect

In deze fase wordt van alle bedrijfsprocessen en technische kwetsbaarheden vastgelegd welke maatregelen **proactief** genomen moeten of kunnen worden om het risico van uitval zo veel mogelijk te beperken. De dit kunnen beleidsmaatregelen zijn en/of technische maatregelen.

Het beleid risicomanagement wordt gebruikt om deze maatregelen in kaart te brengen.

Detect

In deze fase wordt van alle bedrijfsprocessen en technische kwetsbaarheden vastgelegd hoe in de gaten wordt gehouden of een calamiteit zich voordoet.

Respond

In deze fase wordt van alle bedrijfsprocessen en technische kwetsbaarheden vastgelegd hoe gereageerd moet worden indien er zich een calamiteit voordoet.

Recover

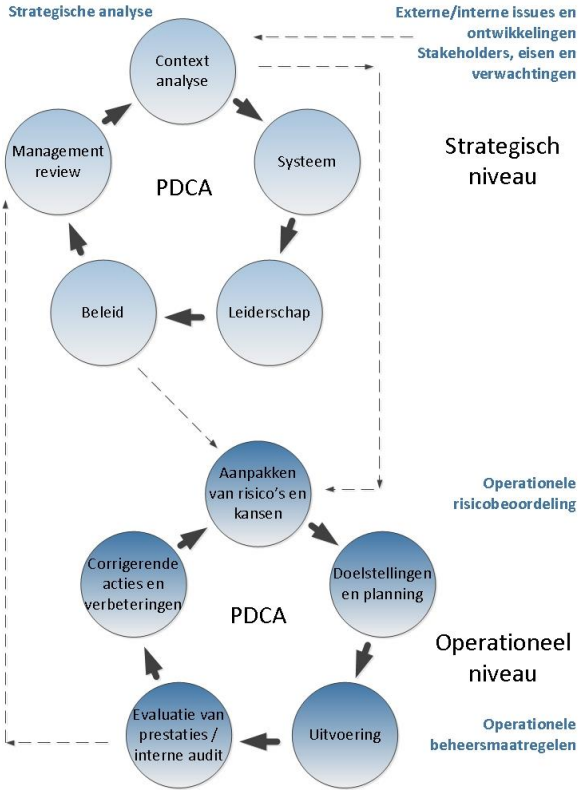
In deze fase wordt van alle bedrijfsprocessen en technische kwetsbaarheden vastgelegd welke herstel activiteiten of herstelscenario's nodig zijn om de het bedrijfsproces of technische kwetsbaarheid te herstellen.

Van alle activiteiten of herstelscenario's dient een werkinstructie geschreven te worden.

3. Beleidsproces voor privacy en informatiebeveiliging

3.1 Overzicht

Binnen het beleidsproces voor privacy en informatiebeveiliging is het belangrijk dat de strategische richting van de organisatie gekoppeld is aan de bedrijfsvoering om ervoor te zorgen dat het managementsysteem (ISMS / PIMS) niet meer in de zijlijn staat van de echte bedrijfsvoering. In de volgende paragrafen worden de twee PDCA-cyclussen toegelicht.



3.2 Contextanalyse

De eerste stap van het beleidsproces voor privacy en informatiebeveiliging bestaat uit twee delen:

- het vaststellen van interne en externe onderwerpen die relevant zijn voor de doelstelling en die het vermogen beïnvloeden om de beoogde resultaten van het managementsysteem (ISMS / PIMS) voor privacy en informatiebeveiliging te behalen;
- inzicht verkrijgen in de belanghebbenden, en de verwachtingen en eisen die zij hebben, die van belang zijn voor het managementsysteem (ISMS / PIMS) voor privacy en informatiebeveiliging.

3.3 Systeem

Dit omvat het toepassingsgebied van het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS) waarin de grenzen en toepasselijkheid van de interne en externe onderwerpen, de verwachtingen en eisen evenals de raakvlakken van activiteiten met de activiteiten van andere organisaties worden vastgesteld.

3.4 Leiderschap

De directie zal leiderschap en betrokkenheid moeten tonen met betrekking tot het managementsysteem (ISMS / PIMS) voor privacy en informatiebeveiliging door:

- het beleid en de doelstellingen vast te stellen en aan te laten sluiten bij de strategische richting van de organisatie;
- het beleid in de organisatie te integreren;
- ervoor te zorgen dat de benodigde middelen beschikbaar zijn om het beleid uit te voeren;
- het belang van een doeltreffend beleid te communiceren;
- ervoor te zorgen dat het beleid zijn beoogde resultaten behaalt;
- mensen aan te sturen en te ondersteunen om bijdrage te leveren aan de doeltreffendheid van het beleid;
- continue verbetering te bevorderen;
- andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebied.

3.5 Beleid

Onderhavig document dat:

- passend is voor het doel van de organisatie;
- beschikbaar is als gedocumenteerde informatie;
- gecommuniceerd wordt binnen de organisatie;
- een verbintenis aan gaat om te voldoen aan de van toepassing zijnde eisen voor privacy en informatiebeveiliging en het continu verbeteren van het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS).

3.6 Directiebeoordeling

Dit is de beoordeling door de directie van het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS) om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen. Het bevat beslissingen met betrekking tot kansen voor verbetering en de noodzaak tot wijziging van het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS). Gedocumenteerde informatie moet bewaard blijven als bewijsmateriaal van de resultaten van de directiebeoordeling. In de beoordeling wordt opgenomen:

- De status van de acties van de voorgaande beoordelingen;

- Wijzigingen in de interne en externe onderwerpen die relevant zijn voor het managementsysteem voor informatiebeveiliging (ISMS / PIMS);
- Feedback over de informatiebeveiligingsprestaties, waaronder; afwijkingen en corrigerende maatregelen, resultaten van monitoren en meten, auditresultaten en of er voldaan is aan informatiebeveiligingsdoelstellingen;
- Feedback van belanghebbenden;
- Resultaten van de risicobeoordelingen en status van het risicobehandelplan;
- Kansen voor continue verbetering.

3.7 Aanpakken van risico's en kansen

De risico's en kansen van de onderwerpen die naar voren gekomen zijn en eisen die gesteld zijn in de contextanalyse worden vastgesteld, beoordeeld en aangepakt. De risicoanalyse wordt gemaakt aan de hand van:

- een risicobeoordelingsprocedure voor privacy en informatiebeveiliging;
- een behandelprocedure voor privacy- en informatiebeveiligingsrisico's. Beheersmaatregelen die hier uit voortkomen moeten passend zijn voor de risicobeoordeling;
- aanvaarding en goedkeuring van het risicoplan door de risico-eigenaren en de acceptatie van de overblijvende privacy- en informatiebeveiligingsrisico's door de directie.

3.8 Doelstellingen en planning

Het vastleggen van relevante privacy- en informatiebeveiligingsdoelstellingen in het risicoplan voor relevante functies en op relevante niveaus. Deze zijn consistent met het privacy- en informatiebeveiligingsbeleid, meetbaar, houden rekening met privacy- en informatiebeveiligingseisen en resultaten van risicobeoordeling en –behandeling, worden gecommuniceerd en geactualiseerd. In de planning van de doelstellingen staat:

- wat er gedaan moet worden;
- welke middelen er nodig zijn;
- wie er verantwoordelijk is;
- wanneer het voltooid moet zijn;
- hoe de resultaten worden geëvalueerd.

3.9 Uitvoering

Aan de hand van de privacy- en informatiebeveiligingsdoelstellingen in het risicoplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. Dit betekent onder andere het opstellen van beleid en werkinstructies voor privacy en informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van management en medewerkers.

3.10 Evaluatie van prestaties/interne audit

Hier wordt vastgesteld door wie, wanneer en wat er gemonitord en gemeten moet worden en met welke methoden. De resultaten worden geanalyseerd en geëvalueerd en bewaard als bewijsmateriaal. De interne audit wordt uitgevoerd om informatie te verkrijgen of het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS) functioneert en overeenkomt met de eisen die gesteld zijn door de organisatie en de (inter)nationale norm(en). Deze audit loopt volgens een vast programma dat regelmatig wordt uitgevoerd en controleert op de doeltreffendheid van het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS).

De organisatie van deze controle en de afspraken voor de bijbehorende rapportage worden in hoofdstuk 4 nader uitgewerkt.

3.11 Corrigerende acties en verbeteringen

Wanneer er uit de evaluatie afwijkingen geconstateerd zijn dan worden die beoordeeld en gecorrigeerd door maatregelen te treffen. Deze maatregelen moeten doeltreffend en passend zijn voor de effecten van de afwijking. Wanneer nodig moeten wijzigingen aangebracht worden in het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS). Documentatie over de afwijking, de genomen maatregelen en de resultaten daarvan moeten bewaard blijven als bewijsmateriaal.

3.12 Cyclisch proces

Het managementsysteem voor privacy en informatiebeveiliging (ISMS / PIMS) is een continu en cyclisch proces. Dit betekent dat op basis van de uitkomst van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn om het privacy- en informatiebeveiligingsbeleid aan te passen of om extra beveiligingsmaatregelen te treffen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen, informatiesystemen of wetgeving aanleiding geven om het privacy- en informatiebeveiligingsbeleid te heroverwegen.

4. Organisatie van privacy en informatiebeveiliging

4.1 Toelichting

In dit hoofdstuk wordt de organisatie van privacy en informatiebeveiliging binnen HealthConnected beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot privacy en informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft. Bovendien levert de toewijzing van taken en verantwoordelijkheden de mogelijkheid om decharge te verlenen voor de uitgevoerde werkzaamheden.
De organisatie van privacy en informatiebeveiliging wordt beschreven volgens de volgende invalshoeken:

- het niveau van de beveiligingstaken, waarbij onderscheid wordt gemaakt naar strategische en operationele informatiebeveiliging;
- rollen en functies voor privacy en informatiebeveiliging binnen de HealthConnected.

Tenslotte wordt in dit hoofdstuk ook aandacht besteed aan de overlegvormen die in het kader van privacy en informatiebeveiliging van belang zijn en aan de manier waarop controle en rapportage is vormgegeven.

4.2 Strategisch en operationeel niveau

In het onderstaande overzicht wordt een indeling van activiteiten met betrekking tot privacy en informatiebeveiliging weergegeven waarbij het niveau van de activiteiten als onderscheidend criterium is gehanteerd.

Niveau	Activiteit	Verantwoordelijkheid	Documentatie
Strategisch	Beleidsvorming	Directie	Privacy- en informatiebeveiligingsbeleid Directiebeoordeling
Operationeel	Planning Uitvoering	Medewerkers	Risicobeoordeling Operationeel beleid per eenheid

Op strategisch niveau vindt de beleidsvorming met betrekking tot privacy en informatiebeveiliging plaats. De directie is verantwoordelijk voor deze beleidsvorming en wordt hierin ondersteund door de CISO. De beleidsvorming wordt vastgelegd in het privacy- en informatiebeveiligingsbeleid.

De planning en uitvoering van activiteiten met betrekking tot privacy en informatiebeveiliging vindt plaats op operationeel niveau. Het managementsysteem (ISMS / PIMS) is het meet- en stuurinstrument dat hierbij wordt ingezet. Verantwoordelijk voor deze activiteiten zijn de CISO en medewerkers.

Ten behoeve van het structureren van de uitvoering van taken met betrekking tot privacy en informatiebeveiliging worden beleid en werkinstructies opgesteld.

4.3 Rollen en functies voor informatiebeveiliging

Alle onderdelen binnen HealthConnected zijn bij privacy en informatiebeveiliging betrokken. In dit privacy- en informatiebeveiligingsbeleid worden de verantwoordelijkheden van de volgende functies en rollen beschreven:

- Directie;
- CISO;
- Medewerkers;
- Functionaris voor de Gegevensbescherming;
- Interne auditor.

4.3.1 Directie

De directie is eindverantwoordelijk voor alle activiteiten binnen HealthConnected en dus ook voor privacy en informatiebeveiliging.

De verantwoordelijkheid voor privacy en informatiebeveiliging omvat:

- het vaststellen van het HealthConnected-brede privacy- en informatiebeveiligingsbeleid;
- het toezien op de naleving van het privacy- en informatiebeveiligingsbeleid door de organisatieonderdelen;
- het evalueren van de toepassing en werking van het privacy- en informatiebeveiligingsbeleid op basis van rapportages over privacy en informatiebeveiliging.

4.3.2 Chief Information Security Officer (CISO)

Alle activiteiten met betrekking tot privacy en informatiebeveiliging worden binnen HealthConnected bewaakt door de CISO. De CISO is dus verantwoordelijk voor de ondersteuning en bewaking van de realisatie en naleving van het privacy- en informatiebeveiligingsbeleid. De CISO is de spin in het web met betrekking tot privacy en informatiebeveiliging binnen

HealthConnected. Tevens vormt de CISO ook het aanspreekpunt inzake privacy en informatiebeveiliging voor de directie en de medewerkers.

De CISO heeft de volgende verantwoordelijkheden:

- beleidsvorming, het beheren van HealthConnected-brede privacy- en informatiebeveiligingsbeleid en het hieruit voortvloeiende onderliggende beleid;
- controle en registratie, het bewaken van het niveau van privacy en informatiebeveiliging binnen HealthConnected;
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van privacy en informatiebeveiliging en het stimuleren van het privacy- en beveiligingsbewustzijn binnen de organisatie;
- evaluatie en advies, het adviseren van de directie en de teamleiders over privacy en informatiebeveiliging en het rapporteren over de status van privacy en informatiebeveiliging binnen HealthConnected.

Daarnaast specifiek over privacy- en informatiebeveiligingsincidenten:

- het verzamelen van informatie over (potentiële) privacy- en informatiebeveiligingsincidenten en -lekken;
- het centraal registreren van (potentiële) privacy- en informatiebeveiligingsincidenten;
- het analyseren en beoordelen van de aard, omvang en oorzaak van privacy- en informatiebeveiligingsincidenten;
- het organiseren van de evaluatie van de afhandeling van privacy- en informatiebeveiligingsincidenten;
- het adviseren van de organisatie over de te nemen preventieve en herstelacties bij privacy- en informatiebeveiligingsincidenten;
- het informeren, instrueren en coördineren van de direct betrokkenen over de uit te voeren preventieve en herstelacties;
- het centraal informeren van gebruikers over (potentiële) privacy- en informatiebeveiligingsincidenten.

4.3.3 Medewerkers

De leidinggevende en de teamleider zijn verantwoordelijk voor de inrichting en uitvoering van privacy en informatiebeveiliging binnen hun bedrijfsprocessen. Zij worden hierbij ondersteund door de CISO. Niet leidinggevende medewerkers zijn verantwoordelijk voor het naleven van beleid en het volgen van werkinstructies binnen hun functie.

Voor alle medewerkers geldt dat zij in hun functieprofiel een verantwoordelijkheid hebben ten opzichte van privacy en informatiebeveiliging wat toegespitst is op de functie. Voorbeelden van verantwoordelijkheden zijn:

- deelnemen aan het IBMF;
- fungeren als voorbeeldfunctie;
- verantwoordelijk voor het risicomanagement;
- verantwoordelijk voor bewustzijn aangaande privacy en informatiebeveiliging;
- positieve en actieve houding ten aanzien van privacy en informatiebeveiliging;
- toezicht houden op de naleving van privacy- en informatiebeveiligingsmaatregelen;
- adviseren bij privacy- en informatiebeveiligingsincidenten;
- medewerking verlenen aan verbeteracties;
- autoriseren van medewerkers;
- privacy en informatiebeveiliging behandelen in werkoverleg en beoordelingen;
- afhandelen van privacy- en informatiebeveiligingsincidenten.

4.3.4 Functionaris voor de Gegevensbescherming (FG)

De taak van de FG is ervoor te zorgen dat de algemene verordening gegevensbescherming nageleefd wordt. De FG speelt een fundamentele rol in het creëren van een cultuur van gegevensbescherming binnen de organisatie en helpt ook bij de implementatie van essentiële elementen uit de algemene verordening gegevensbescherming, zoals:

- de beginselen van gegevensverwerking;
- de rechten van de betrokkenen;
- gegevensbescherming door ontwerp;
- gegevensbescherming door standaardinstellingen;
- register van verwerkingsactiviteiten;
- beveiliging van de verwerking;
- melding van en communicatie over inbreuken met betrekking tot gegevens.

De FG dient naar behoren en tijdig te worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Alle relevante informatie moet tijdig aan de FG worden bezorgd, zodat de FG passend advies kan verlenen. De FG geeft een advies en doet aanbevelingen wanneer beslissingen worden genomen die gevolgen hebben voor de gegevensbescherming. Wanneer het advies of aanbeveling van de FG niet wordt overgenomen zal de redenen voor het niet volgen van het advies of aanbeveling door de FG worden gedocumenteerd.

In het geval van het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) dient informatie ingewonnen te worden bij de FG. De FG dient advies te verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en ziet erop toe dat de uitvoering daarvan in overeenstemming is met de AVG.

De FG is het aanspreekpunt voor klanten (aangaande vraagstukken over gegevensbescherming) en contactpersoon van de toezichthoudende autoriteit. De FG is gehouden aan geheimhouding en vertrouwelijkheid overeenkomstig het Unierecht of lidstatelijk recht. In dit kader heeft de FG de volgende taken:

- meewerken aan het creëren van een cultuur van gegevensbescherming;
- informatie verzamelen om verwerkingsactiviteiten te identificeren;
- de naleving van verwerkingsactiviteiten analyseren en controleren;
- de verwerkingsverantwoordelijke of de verwerker informeren, adviseren en aanbevelingen doen;
- redenen voor het niet opgevolgd advies of aanbeveling documenteren;
- adviseren en assisteren bij het uitvoeren van een gegevensbeschermingseffectbeoordeling;
- klanten te woord staan met vragen over gegevensbescherming;
- samenwerken met toezichthoudende autoriteit (contactpersoon).

De FG mag binnen HealthConnected geen functie bekleden waarbij hij of zij de doelstellingen van en de middelen voor de verwerking van persoonsgegevens moet bepalen.

4.3.5 Interne auditor

HealthConnected voert jaarlijks interne audits uit. Een interne audit is een onderzoek dat, met een systematische en gedisciplineerde aanpak, wordt uitgevoerd naar het goed en betrouwbaar functioneren van de interne organisatie door (interne) auditors die in dienst zijn van die organisatie of extern wordt ingehuurd. In het geval van HealthConnected is gekozen om de

interne audit te laten uitvoeren door een externe auditor. De auditor van HealthConnected richt zich op de normen ISO 27001, NEN7510 en ISO 27701.

4.4 Overlegvormen voor informatiebeveiliging

Voor overleg, coördinatie en afstemming op het gebied van privacy en informatiebeveiliging worden de volgende overlegvormen onderscheiden:

- Bilateraal overleg directie en CISO;
- IBMF (informatiebeveiligingsmanagementforum) onder leiding van CISO.

4.4.1 Bilateraal overleg directie en CISO

De directie en de CISO overleggen regelmatig bilateraal over privacy en informatiebeveiliging. In dit overleg wordt aandacht besteed aan kwartaalrapportages, voorstellen voor de directie, voorstellen voor wijzigingen van het privacy- en informatiebeveiligingsbeleid, investeringsvoorstellen voor privacy- en beveiligingsmaatregelen, etc. Dit overleg wordt minimaal tweemaal per jaar gehouden.

4.4.2 IBMF

De CISO voert overleg met key medewerkers van de afdelingen Beheer, Ontwikkeling, Business- & Accountmanagement en Support in het IBMF. Het overleg vindt plaats op maandelijkse basis en kent een standaard agenda. Het IBMF heeft de taak om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor privacy- en beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie. De taken van het IBMF zijn:

- Privacy- en informatiebeveiligingsincidenten van de afgelopen maand
    - Bespreken of gedachte wisselen over belangrijke privacy- en informatiebeveiligingsincidenten van de afgelopen maand. Zijn er incidenten die vaker terugkomen? Zo ja, dan 'problem' van maken.
- Nieuwe ontwikkelingen (security by design / privacy by design / communicatie)
    - Uit de NEN 7510: Er moet een formele verklaring van het toepassingsgebied worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen. In dit overleg dient iedereen vanuit zijn vakgebied nieuwe ideeën over ontwikkelingen in te brengen zodat de andere verantwoordelijken op de hoogte worden gesteld en vanuit hun vakgebied vragen kunnen stellen en/of input te leveren zodat zij hun verantwoordelijkheid ook echt kunnen nemen.
- Status IB-acties
    - Iedereen bekijkt voor de bijeenkomst zijn/haar eigen IB-acties. Wanneer er acties bij zitten die niet individueel opgelost kunnen worden dan worden deze in dit overleg ingebracht.
- Communicatie en voorlichting
    - Coördineren van de implementatie van het gewenste niveau van privacy en informatiebeveiliging en het stimuleren van het privacy- en informatiebeveiligingsbewustzijn binnen de organisatie. Wat zijn de wensen van de teamleiders hierin?

4.5 Controle en rapportage over informatiebeveiliging

Met betrekking tot privacy en informatiebeveiliging worden de volgende controlevormen onderscheiden:

- operationele controle op de naleving van het privacy- en informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen;

- controle op de voortgang van de implementatie en borging van het privacy- en informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen;
- onafhankelijke controle.

De operationele controle op de naleving van beleid en richtlijnen wordt verricht door de leidinggevenden en de teamleider(s). Zij rapporteren aan de CISO over de voortgang van de implementatie van informatiebeveiliging binnen de eigen afdeling (gerapporteerd in privacy- en informatiebeveiligingsacties, privacy- en informatiebeveiligingsacties incidenten & IBMF). Hierbij wordt de voortgang afgezet tegen de gemaakte afspraken.

Controle op de voortgang gebeurt op kwartaalbasis. De CISO verzamelt de rapportages van de afdelingen. Van deze verschillende rapportages en andere interne/externe factoren wordt een geconsolideerde voortgangsrapportage gemaakt (de kwartaalrapportage). Deze rapportages wordt door de CISO besproken met de directie op het directieoverleg. Van het directieoverleg wordt een verslag gemaakt (de directiebeoordeling) waarin sturing en verbeteringen worden opgenomen alsmede het wijzigen van strategie en beleid. De CISO zorgt voor het doorvoeren van genoemde zaken in het managementsysteem (ISMS / PIMS).

Onafhankelijke controle (interne audit) met betrekking tot privacy en informatiebeveiliging wordt uitgevoerd door een externe auditor. Deze auditor stemt de planning van zijn activiteiten af met de CISO. De CISO wordt over de uitkomsten van de controles geïnformeerd.

Akkoord directie, 25-01-2023
Paul Witteman