Beleid Informatiebeveiliging MCB en HN

1 Inleiding

De huisarts van tegenwoordig is steeds meer de eerstelijns regisseur van de zorgverlening gericht op de individuele patiënt, zodat deze steeds meer zelf de verantwoordelijkheid kan nemen voor zijn gezondheid. Dit brengt dus vooral ook heel veel communicatie met zich mee.

Medical Connect Beheer BV (MCB) is met één werkmaatschappij actief in de Health Care branche, te weten Huisartsendienst NL BV (HN). Deze bedrijven hebben gemeenschappelijk dat ze met en/of over personen (patiënten/cliënten) communiceren. Dit brengt met zich mee dat er vertrouwelijke persoonsgegevens verwerkt worden. Genoemde bedrijfsonderdelen worden verder in dit stuk als de organisatie benoemd.

Uiteraard moet deze communicatie niet alleen efficiënt worden uitgevoerd maar brengt deze ook privacy risico's met zich, die voor een individuele huisarts moeilijk zijn af te dekken. In de Algemene Verordening Gegevensbescherming (AVG) is vastgesteld dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen dienen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De organisatie wil de huisarts hierin ontzorgen door het verzorgen van deze communicatie, waarbij ze aanspreekbaar is op fouten, die tijdens dit communicatieproces worden gemaakt. Om dit aantoonbaar en controleerbaar te maken is de dienstverlening conform de normen voor informatiebeveiliging ingericht en worden er specifieke verwerkersovereenkomsten afgesloten. Ook wordt er zoveel mogelijk gewerkt met hiertoe gecertificeerde en genormeerde subverwerkers, zoals ICT-dienstverleners, verzendhuizen en agendabouwers.

Informatiebeveiliging is geen doel op zich, maar dient uitsluitend het belang van de organisatie, haar opdrachtgevers en diens cliënten/relaties. De continuïteit, kwaliteit en vertrouwelijkheid van bedrijfsprocessen staan centraal, evenals respect voor de privacy van alle betrokkenen. De uitgangspunten van de organisatie zijn vastgelegd en worden gedragen door de directie en, afgeleid daarvan, door de hele organisatie.

Er worden enerzijds duidelijke keuzes gemaakt in beveiligingsmaatregelen en anderzijds wordt de toepassing daarvan ook gecontroleerd ter continue verbetering van zowel beleid als uitvoering. Het doel hierbij is niet om toe te werken naar een maximaal beveiligingsniveau, maar naar het instant houden van het door het management beoogde niveau van informatiebeveiliging.

2 Verantwoordelijkheid, doelstelling en doelgroep

Bedreigingen van een veilige en betrouwbare informatievoorziening kunnen fysiek van aard zijn, zoals brand en wateroverlast. Maar ook technisch, bijvoorbeeld in de vorm van

storingen in programmatuur, apparatuur of de stroomvoorziening. De informatievoorziening kan ook worden bedreigd door (on)opzettelijke fouten en vergissingen of door opzettelijke kwaadaardige acties zoals hacking, phishing, computerfraude, etc.

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die de informatievoorziening van de organisatie kunnen schaden, te voorkomen en/of de kans verkleinen en/of eventuele gevolgen te beperken. Gelet op de mogelijke impact van verstoringen op de bedrijfsvoering en continuïteit van de organisatie en haar klanten berust eindverantwoordelijkheid voor het beleid inzake informatiebeveiliging bij de directie van de organisatie.

Het Beleidsdocument Informatiebeveiliging (hierna te noemen beleid IB) maakt deel uit van het algehele beveiligingsbeleid van de organisatie. De doelstelling van het beleid IB inzake de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening van de organisatie luidt:

> 'Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de informatievoorziening te beschermen tegen interne en externe bedreigingen'.

De organisatie neemt hierin eveneens de volgende subdoelstellingen mee:
-Het waarborgen van de continuïteit van het primaire proces;
-Het beschermen van vertrouwelijke en/of gevoelige informatie in het primaire proces;
-Het voorkomen van imagoschade en het behouden van een professionele uitstraling;
-Het voorkomen van bedrijfsschade;
-Het beschermen van vitale bedrijfsinformatie en informatie van haar klanten;
-Het voldoen aan wettelijke voorschriften.

Met nadruk wordt gesteld dat het preventieve aspect van het allergrootste belang is. Voorkomen is in het algemeen beter dan genezen.

Algemene en specifieke verantwoordelijkheden voor informatiebeveiligingsbeheer, zoals beleid, planning en control, zijn toegekend aan gedefinieerde rollen. De organisatie heeft ook een Functionaris Gegevensbescherming aangewezen. Daarnaast beschikt de organisatie over een privacyreglement dat ook op haar websites gepubliceerd is. Alle leidinggevenden dienen ervoor zorg te dragen, dat aan de in dit beleid IB geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijzen en de daarbij gehanteerde informatiesystemen.

3 Toepassingsgebied

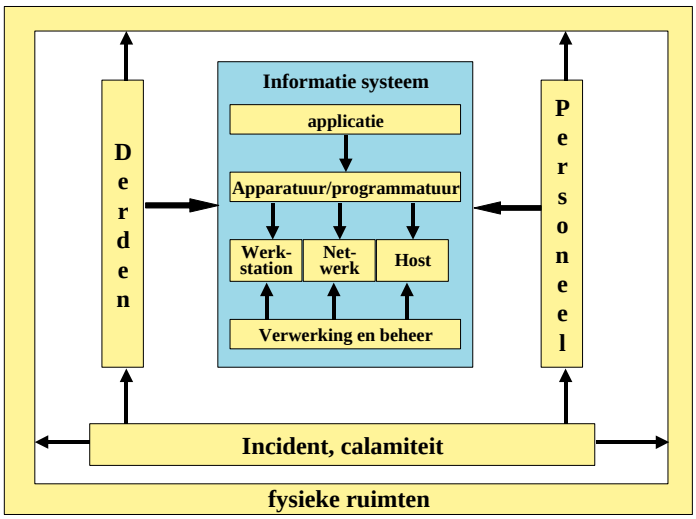
Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard (verwerkt) wordt in de dienstverlening van de organisatie aan klanten en de daarmee samenhangende contractuele verplichtingen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers en inhuur/contractanten van de organisatie. Afwijkingen hierop dienen te worden gemeld, zodat het management systeem continu verbeterd kan worden. Daarnaast geldt dit beleid ook voor leveranciers, die de organisatie ondersteunen bij

haar dienstverlening aan klanten. De ethische code (en geheimhoudingsverklaring) van de organisatie vormt een onlosmakelijk onderdeel van dit beleid.

3.1 Houderschap en reikwijdte van het beleid

De organisatie is dus verantwoordelijk voor het beschikbaar stellen van haar dienst met voldoende beveiligingsopties, zodat haar klanten kunnen voldoen aan de voor haar geldende IB-normen en andere wet- en regelgeving. Dit ontslaat echter de klant niet van de eindverantwoordelijkheid voor de beveiliging van haar informatievoorziening. ICT en systeembeheer is geoutsourcet en wordt verzorgd door Techni Team ICT, dat ISO 27001 & NEN 7510 gecertificeerd is. Als extern bedrijf legt Techni Team ICT verantwoording af aan de organisatie.

Van elk informatiesysteem, inclusief de daarbij behorende gegevens, is expliciet één houder benoemd in het bedrijfsmiddelenregister. Het houderschap impliceert de eindverantwoordelijkheid voor het betreffende systeem, inclusief het bepalen van bij het systeem te onderkennen risico's, het classificeren van het systeem en de daarbij behorende gegevens en het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen. Naast de applicatie betreft dit ook de juiste inzet van de infrastructurele componenten (werkstations, servers en het interne en externe netwerk), de juiste verwerking, het adequate beheer, het goed functioneren van het personeel, het maken van afspraken met derden, fysieke beveiliging en voorzieningen om incidenten en calamiteiten te voorkomen of af te handelen. In onderstaand figuur zijn alle genoemde deelgebieden van een informatiesysteem opgenomen.



Er wordt gesproken over eindverantwoordelijk omdat een aantal aspecten van het informatiesysteem uitbesteed worden aan subverwerkers.

De organisatie beschouwt informatiebeveiliging al jarenlang als een belangrijk issue, waarbij zeker gesteld moet worden dat risico's voor de klant acceptabel zijn en dat maatregelen werkend gemaakt moeten worden zonder dat dit ten koste gaat van de effectiviteit, flexibiliteit en efficiency van de dienstverlening.

Het is nadrukkelijk niet de ambitie van de directie om een eerste klasse speler op informatieveiligheid te worden. We streven daarbij dus geen maximaal beveiligingsniveau na, maar een passend niveau van beheersmaatregelen, zodat de organisatie haar diensten flexibel kan blijven aanbieden tegen acceptabele kosten.

Dit passend niveau wordt bereikt door een zorgvuldige afweging van kosten en baten. De te nemen maatregelen moeten daarom worden afgestemd op de risico's, waarbij een zorgvuldige afweging wordt gemaakt tussen privacy, optimale veiligheid, praktische haalbaarheid en werkbaarheid. Dit is vaak situatie afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld.

In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het mitigeren van de risico's disproportioneel hoog zijn. Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

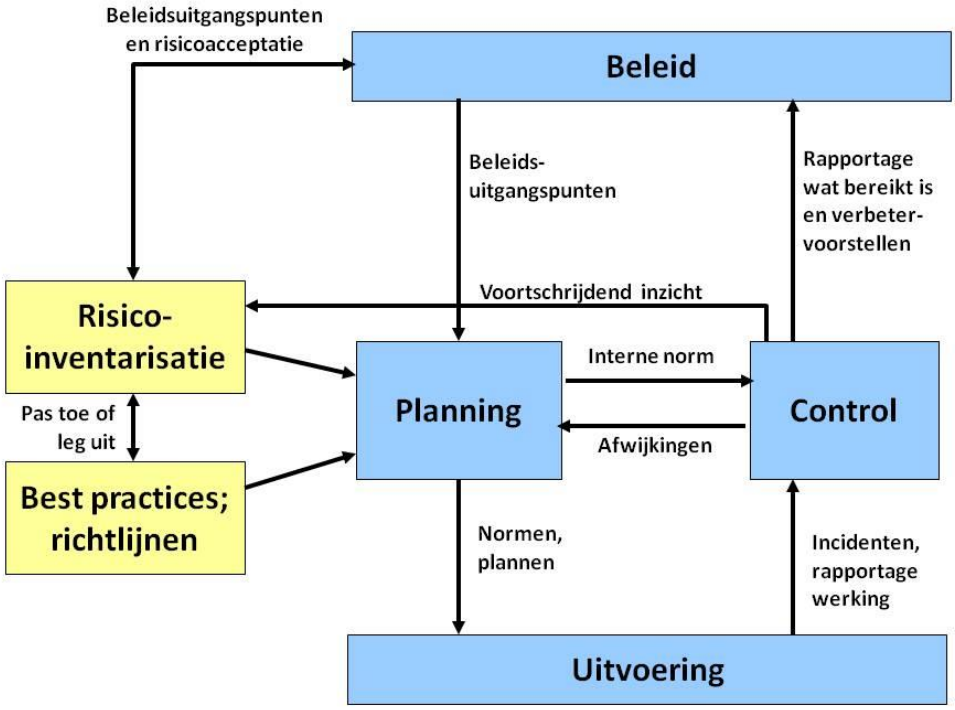
Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van de organisatie met anderen. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

3.2 Uitwerking van dit beleid

Op basis van dit beleid worden risico analyses uitgevoerd en wordt een set van maatregelen en controls gedefinieerd als basisbeveiligingsniveau (BBN), dat geldt als minimum voor de dienstverlening aan klanten. Op verzoek van stakeholders kan ook een hoger niveau van beveiliging worden overeengekomen, na vastlegging in wijzigingsprocedure en overeenkomsten.

3.3 Controle werking en naleving van het beleid

Jaarlijks wordt de werking en de naleving van het beleid intern geëvalueerd en hierover wordt gerapporteerd aan de directie. Onderdeel van deze evaluatie zijn het opnieuw beoordelen van risico's en een impact analyse van nieuwe wet- en regelgeving. Onderdeel van deze rapportage is ook een plan met verbetervoorstellen. De directie beoordeelt de rapportage, keurt voorstellen al dan niet goed en kent budget toe voor de realisatie van de voorstellen. Onderstaand is dit schematisch weergegeven.



Certificering, normering en accreditatie zijn een verschijnsel dat de hele zorg sinds een jaar of acht in de greep houdt. Hoewel certificering, normering en accreditatie niet wettelijk verplicht is, stellen klanten bij hun inkoop soms eisen op dit gebied. Voor de organisatie, een strategisch partner in de zorg sector, is het van essentieel belang dat haar klanten, medewerkers en andere partners kunnen vertrouwen op een veilige manier van informatieverwerking. Omdat DMDR, marktleider in medische (vaccinatie) post, onderdeel uitmaakte van de organisatie, was ISO 27001 certificering & NEN 7510 normering in 2016 een logisch gevolg. ISO 27001 is de internationale standaard voor informatiebeveiliging management, gericht op het continue managen, beheren en verbeteren van informatiebeveiliging risico's. De NEN 7510 is een vergelijkbare norm voor de zorg. Hierin worden met name aanvullende eisen gesteld rondom gezondheidsinformatie. De NEN 7510 is bedoeld voor zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie.

Middels jaarlijkse externe audits toonde de organisatie aan dat ze voldeed aan deze strenge normen voor informatiebeveiliging. In 2019 heeft de organisatie, als een van de eerste partijen in Nederland, succesvol de transitie van NEN 7510:2011 naar NEN 7510:2017 uitgevoerd en is de hercertificeringsaudit met positief resultaat afgerond. De laatste controleaudit op 14 en 15 december 2021, door de externe auditor BSI, toonde aan dat de organisatie op een bijzonder mature manier met de eisen van de standaard omgaat: 'De borging van informatieveiligheid is gestoeld op informatie die zo recent is als het risicoacceptatie-niveau dat toelaat, en dat is exact de bedoeling: weten dat de maatregelen daadwerkelijk doen wat ze moeten doen. Als kans voor verbetering wordt de ISO 27007:2020 aanbevolen om nog beter de eisen van de ISO 27001 te interpreteren en te auditeren. De eisen van de norm zijn in de processen van de organisatie geïntegreerd en geborgd, zo blijkt na audit van niet-ICT operationele processen. Een ander sterk punt zijn de continue trainingen in bewustzijn rond de problematiek van informatie- en cyberveiligheid: "bewustzijn leer je niet aan, maar kweek je." Er werden geen afwijkingen genoteerd, en de enige open afwijking werd gesloten na bewijs van de het resultaat van de correctieve maatregel'.

De scope (toepassingsgebied) van deze certificering van ISO 27001 & NEN 7510 betrof: het in zorgprojecten regisseren van onderzoeken en diagnosticeren van medische aandoeningen en hierover rapporteren.

De organisatie voelt zich echter eind 2022 gedwongen om haar ISO 27001 certificering & NEN 7510 normering op vrijwillige basis te schorsen voor de gehele scope. Ze ziet zich hiertoe genoodzaakt om de volgende redenen:

A. Afsplitsing DMDR, marktleider in medische (vaccinatie) post, van de organisatie;
B. De onzekerheid over de contractering van haar zorgaanbod door zorgverzekeraars;
C. Het omlaag brengen van de directe administratielast voor de kleine organisatie;
D. Het omlaag brengen van de directe en indirecte kosten voor de kleine organisatie;
E. De beperkte toegevoegde waarde van accreditatie, certificering en normering voor de cliënten zoals blijkt uit recent klanttevredenheidsonderzoek.

De leden van de RvT van stichting DCT hebben geconcludeerd dat certificering van DCT (en HN) wat hen betreft niet langer nodig is wanneer gewerkt wordt met gecertificeerde onderaannemers voor wat betreft patiënten communicatie, ICT en dergelijke.

4 Beleidsuitgangspunten

In deze beleidsuitgangspunten geeft de directie aan op welke wijze zij wil dat de informatiebeveiliging vorm gegeven wordt, passend bij de organisatie en bovengenoemde doelstellingen. Bij de verdere invulling van dit beleid dienen de volgende uitgangspunten gehanteerd te worden:

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor de organisatie. De directie stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast en beoordeelt periodiek de werking van het beleid en de naleving van deze maatregelen intern om te borgen, dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. De organisatie conformeert zich m.b.t. de informatiebeveiliging en privacy aan de van toepassing zijnde wetgeving.
3. De organisatie streeft er naar om haar dienstverlening aan klanten continu te verbeteren.
4. Indien de privacy van een individu of een kleine groep cliënten of patiënten risico’s met zich meebrengt voor het zorgproces, dan prevaleert het borgen van een adequaat zorgproces boven de privacy.
5. De organisatie beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.
6. Vertrouwen is voor de organisatie een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. De organisatie gaat er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.
7. Het HRM-beleid is mede gericht op het verbeteren van de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening bij medewerkers.

8. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
9. Aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.
10. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
11. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers en andere betrokkenen te waarborgen.
12. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van de organisatie.
13. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.
14. De organisatie en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
15. Input van klanten die vertrouwelijke data bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.
16. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
17. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productieomgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden.
18. Productieomgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
19. Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
20. Er zijn functiescheidingen aangebracht tussen de beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
21. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
22. Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de informatievoorziening te waarborgen.
23. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
24. Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor de organisatie wettelijk en/of contractueel verantwoordelijk is.

De voltallige directie van de organisatie, bestaande uit de bovengenoemde bedrijfsonderdelen, is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid op 18 oktober 2022 vastgesteld.