Beleid Informatiebeveiliging MCB

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. MCB ondersteunt huisartsen in de routinematige communicatie met de betrokkenen variërend van uitnodigingen voor een griepprik tot en met het communiceren van uitslagen van onderzoeken, die in opdracht van de huisarts door ZBC's en/of Huisartsenlaboratoria worden uitgevoerd.

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. MCB wil de huisarts hierin ontzorgen door het verzorgen van deze communicatie, waarbij MCB aansprakelijk is voor fouten, die tijdens dit communicatieproces worden gemaakt. Om dit aantoonbaar en controleerbaar te maken heeft de directie van MCB zich ten doel gesteld haar dienstverlening conform NEN-ISO/IEC 27001 en NEN 7510 in te richten en zich te laten certificeren, zodat aan die behoefte van klanten wordt voldaan.

2 Verantwoordelijkheid, doelstelling en doelgroep

Gelet op de mogelijke impact van verstoringen op de bedrijfsvoering en continuïteit van MCB en haar klanten berust eindverantwoordelijkheid voor het beleid inzake informatiebeveiliging bij de directie van MCB.

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

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, werkwijze en de daarbij gehanteerde informatiesystemen.

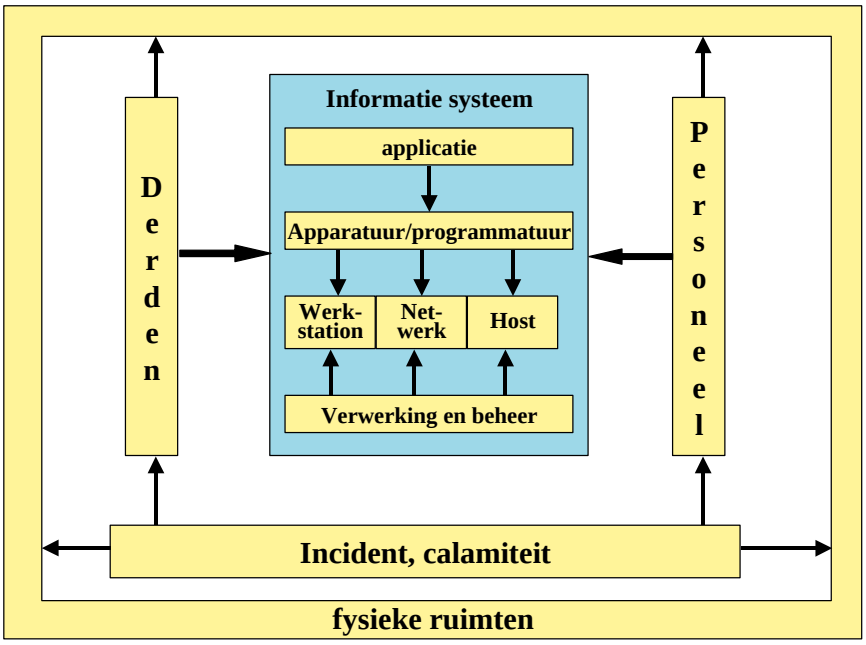
3 Toepassingsgebied

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van MCB aan klanten en de daarmee samenhangende contractuele verplichtingen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van MCB. Afwijkingen hierop moeten gemeld worden, zodat het management systeem continu verbeterd kan worden. Daarnaast geldt beleid ook voor contractanten, die MCB ondersteunen bij haar dienstverlening aan klanten. De ethische code van MCB vormt een onlosmakelijk onderdeel van dit beleid.

3.1 Houderschap en reikwijdte van het beleid

MCB 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. Ook voldoet de hosting en het beheer van de software aan deze eisen. Dit ontslaat echter de klant niet van de eindverantwoordelijkheid voor de beveiliging van haar informatievoorziening.

Van elk informatiesysteem, inclusief de daarbij behorende gegevens, dient expliciet één houder te zijn benoemd. 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 andere houders zoals MCB.

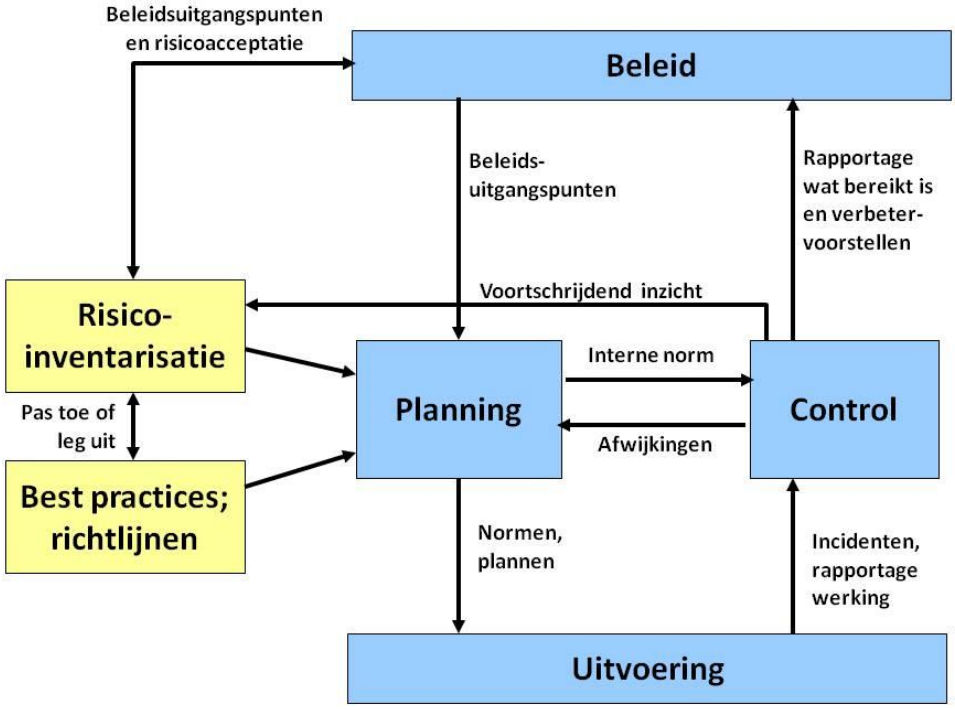
Hierbij wordt niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau, zodat MCB haar diensten kan bieden tegen een acceptabele kosten.

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. In overleg kan een hoger niveau van beveiliging met een klant worden afgesproken.

3.3 Controle werking en naleving van het beleid

Halfjaarlijks 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.



Daarnaast wordt jaarlijks een audit uitgevoerd door een onafhankelijke derde partij, die hiertoe bevoegd en deskundig is. De rapportage hiervan is beschikbaar voor (potentiële) klanten.

4 Beleidsuitgangspunten

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

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor MCB. De directie stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om te borgen, dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. MCB conformeert zich m.b.t. de informatiebeveiliging en privacy aan de van toepassing zijnde wetgeving.
3. MCB streeft er naar om haar dienstverlening aan klanten continu te verbeteren.
4. De doelstellingen en beheersmaatregelen van de normen NEN-ISO/IEC 27001, NEN 7510 en de privacy richtsnoeren van de AP vormen, voor zover zij bijdragen aan de informatiebeveiliging en de beveiliging van persoonsgegevens van MCB, het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
5. 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.
6. MCB 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..
7. Vertrouwen is voor MCB een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. MCB gaat er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.
8. Het HRM-beleid is mede gericht op het verbeteren van de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening bij medewerkers. Tijdens een jaarlijkse evaluatie wordt dit aan de orde gesteld.
9. 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.
10. 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.
11. 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.
12. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers en andere betrokkenen te waarborgen.

13. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van MCB.
14. 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.
15. MCB en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
16. Input van klanten die vertrouwelijke data bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.
17. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
18. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productie omgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden.
19. Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
20. Het beheer en de opslag van gegevens in productie omgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
21. Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
22. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
23. Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de informatievoorziening te waarborgen.
24. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
25. MCB implementeert die aanvullende maatregelen, zodat zij voldoet aan NEN 7510.
26. Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor MCB wettelijk en/of contractueel verantwoordelijk is.

Aldus overeengekomen en in drievoud ondertekend en geparafeerd door de voltallige directie

Plaats: Ridderkerk

Datum: 24 aug 2017

Ruud Boonman	Martin ten Cate	René den Otter
Directeur	Directeur	Directeur