Informatiebeveiliging en Privacy; beleid CHD 2018-2020

Vastgesteld MT 19 december 2017

Centrale Huisartsendienst Drenthe

Stichting Centrale Huisartsendienst Drenthe
Postbus 409
9400 AK Assen

1 Inleiding

De CHD is een zorginstelling die werkt met zeer privacygevoelige gegevens van patiënten, zorgverleners en personeel. Gegevens over de gezondheidstoestand van mensen worden door de wetgever als van de een na hoogste categorie van vertrouwelijkheid beschouwd. Vanuit de wet ligt bij de CHD dus een grote maatschappelijke verantwoordelijkheid ervoor te zorgen dat de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de verwerkte gegevens ten allen tijde is gewaarborgd.

Binnen de CHD zijn meer dan 300 zorgverleners en medewerkers werkzaam op verschillende locaties en in hun werk is veilig gebruik kunnen maken informatie een noodzaak. De kwaliteit van de zorgverlening is er direct van afhankelijk. Het verlies van gegevens, uitval van ICT en/of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de patiëntenzorg. En kunnen leiden tot imago- en financiële schade.

Informatiebeveiliging (IB) is het proces dat deze belangen dient. Met de invoering van nieuwe wetgeving in de vorm van de Algemene Verordening Gegevensbescherming en de aanvullende eisen die daarin gesteld worden is het goed het Informatiebeveiligingsbeleid (IBB) van de CHD te actualiseren. In dit document wordt het beleid verder uitgewerkt.

2 Waar willen we heen? Welke uitgangspunten horen daarbij?

De CHD staat ervoor dat patiënten bij haar in goede handen zijn. Dat stelt hoge eisen aan de kwaliteit van zorgverlening maar zeker ook aan de kwaliteit van de hulpmiddelen en de processen die daarbij een rol spelen. Patiënten mogen én moeten er zonder meer op kunnen vertrouwen dat de informatie die bij de zorgverlening van belang is, beschikbaar is op het moment dat die nodig is, dat de informatie juist en volledig is en dat die informatie goed beveiligd is zodat alleen diegene er kennis van neemt die dat ook in de context van de hulpvraag moet doen.

Wat geldt voor patiënten in het primair proces geldt net zo voor huisartsen, medewerkers en andere betrokkenen. Ook bij de ondersteunende processen wil de CHD de beschikbaarheid, integriteit en vertrouwelijkheid van informatie gewaarborgd hebben.

De CHD stelt zich met het IB-beleid ten doel:

- Het garanderen van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de door CHD verwerkte persoonsgegevens en andere voor de bedrijfsvoering relevante informatie
- Het zo veel als mogelijk beperken van de gevolgen van eventuele beveiligingsincidenten en datalekken
- Het invullen van rechten van betrokkenen op het gebied van privacy
- Het naleven van de relevante wet- en regelgeving

Uitgangspunten voor het IB-beleid zijn:

- Passend binnen relevante wettelijke en andere kaders, zoals de WGBO, Wbp, NEN7510 en andere voor de gezondheidszorg gebruikelijke (medisch inhoudelijke) normen
- Toetsing van de uitvoering van het IBB heeft een plaats in de directiebeoordeling zoals die in de structuur van HKZ periodiek door CHD wordt uitgevoerd
- Er ligt een expliciete verbinding met de PDCA cyclus van ons Risico management

- De toegevoegde waarde van de maatregelen, de kosten en de risico's staan in redelijke verhouding tot elkaar staan
- CHD streeft niet naar certificering voor NEN 7510 of een andere norm op het gebied van IB

3 Waar hebben we het eigenlijk over?

Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Van eerste vastlegging tot aan geprotocolleerde vernietiging. Over welke informatie we het hebben is in detail uitgewerkt in het Verwerkingenregister van de CHD, inclusief classificatie en rondslag voor verwerking.

Het IB-beleid van de CHD is in ieder geval van toepassing op:

Processen
Primaire proces: de zorgverlening op de huisartsenspoedposten door huisartsen, assistentes en verpleegkundige, daaronder begrepen de aanname van telefonische oproepen op de posten en het afleggen van visites bij patiënten thuis.
Ondersteunende processen: HRM, contractbeheer zorgverleners, applicatie- en systeembeheer ICT, financieel beheer, roostering, algemeen management. Hieronder wordt nadrukkelijk ook begrepen het terugluisteren van gesprekken in het kader van personeelsontwikkelingsbeleid en van afhandeling van klachten.

Gegevens
Primaire proces: (medische) patiëntgegevens uit de eigen medische registratie en de regionale patiëntenindex ten behoeve van de uitwisseling van medische gegevens met externe registraties
Ondersteunende processen: personeelsgegevens, gegevens met betrekking tot gebruik en inrichting van de ICT-voorzieningen, gegevens met betrekking tot zorgverleners, financiële gegevens en overige gegevens.

Voorzieningen
ICT-applicaties en -systemen (vast en mobiel), elektronische communicatie infrastructuur voor informatie-uitwisseling, digitale en niet-digitale archieven en overige informatie-voorzieningen.

Locaties
De huisartsenposten in Assen, Emmen, Hoogeveen en Meppel
De auto's waarmee de huisartsen visites afleggen
Het kantoor in Assen (Oostersingel)
De serverruimte van de CHD in het WZA en andere ruimtes bij derden die deel uitmaken van de informatievoorziening van de CHD.

Cloudoplossingen
Gegevensverwerkingen die op een locatie worden uitgevoerd door een andere partij waarop de CHD geen directe uitvoerende zeggenschap heeft (cloudoplossingen)

4 Aanpak

Bij de aanpak hanteren we de systematiek van de Demming circle: een gestructureerde PDCA cyclus die voortdurend wordt doorlopen om steeds verder te verbeteren. Beleid formuleren, aan de hand van

een gedegen risico analyse in kaart brengen welke risico's het realiseren van het beleid kunnen frustreren, acteren naar de conclusies van de analyse, check op verbetering, heroverwegen beleid obv nieuwe inzichten en ervaringen. En weer een risico analyse, etc. De cyclus willen we eenmaal per jaar geheel doorlopen.
Deze aanpak is niet uniek en wordt ook op andere deelgebieden toegepast. Uiteindelijk komt alles samen in ons Risicomanagement en daar moet ook deze cyclus een plek krijgen, net als bij voorbeeld de cyclus die in de context van de HKZ certificering wordt doorlopen. In die context komt Informatiebeveiliging dan ook aan de orde in de jaarlijkse directiebeoordeling. Verder is het een onderwerp in de jaarlijkse bespreking van Risicomanagement in de Raad van Toezicht van CHD.

5 Organisatie, betrokkenen en taken

Voor de voorbereiding en uitvoering van het IB-beleid en alle ondersteunende informatie-beveiligingsmaatregelen benoemt de CHD een verantwoordelijke, de functionaris IB. Deze verantwoordelijke coördineert alle benodigde werkzaamheden om het IB-beleid te realiseren en dient binnen alle geledingen van de CHD-organisatie als zodanig bekend te zijn gemaakt. Periodiek, minstens tweemaal per jaar, rapporteert de functionaris IB over de voortgang van de realisatie van het beleid aan het MT. En eenmaal per jaar, in de context van Risicomanagement, aan de RvT.

De functionaris IB beschikt over bevoegdheden die hem of haar in staat stellen de taken op het terrein van de informatiebeveiliging te kunnen vervullen. Daaronder vallen in ieder geval:

- het geven van aanwijzingen aan medewerkers en zorgverleners ten aanzien van de uitvoering van het IB-beleid
- het instellen van werkgroepen of het inzetten van medewerkers ter ondersteuning van de uitvoering van zijn/haar taken in het kader van het IB-beleid.

In het licht van de AVG zal de CHD uiterlijk vanaf mei 2018 beschikken over een Data Protection Officer, deze rol is verplicht voor ondermeer organisaties die medische gegevens verwerken. Aan deze rol worden door de wet eisen gesteld, wanneer intern invullen niet haalbaar is kan ook externe inhuur van deze rol worden overwogen.

Verdeling van taken en verantwoordelijkheden rond IB
De CHD stelt de verantwoordelijkheden ten aanzien van IB vast. Op hoofdlijn:

Taken	Verantwoordelijke(n)
Besluitvorming IB-beleid	Directie/MT
Onderhouden en evalueren van het IB-beleid	Functionaris IB
Risico- en afhankelijkheidsanalyses uitvoeren	Functionaris IB
Voorbereiden te nemen maatregelen in het kader van IB	Functionaris IB
Besluitvorming te nemen maatregelen in het kader van IB	Directie/MT
Invoeren, onderhouden en evalueren maatregelen in het kader van IB	Functionaris IB, lijnmanagement, applicatie- en systeembeheer
Rapporteren en evalueren van Informatiebeveiliging incidenten	Functionaris IB, lijnmanagement
Uitdragen van het IB-beleid	Directie, lijnmanagement
Kennis van het IB-beleid	Alle medewerkers en

	zorgverleners
Uitvoeren van de bij de eigen functie behorende maatregelen in het kader van IB	Alle medewerkers en zorgverleners

6 Aanpak in de praktijk

In het voorjaar van 2017 is de eerste risico analyse op het gebied van IB uitgevoerd, met externe begeleiding. De bevindingen en daaruit voortkomende activiteiten zijn geprioriteerd en uitgewerkt in een plan van aanpak dat in juli 2017 door het MT van de CHD is geaccordeerd. Bij de uitvoerende activiteiten zijn meerdere medewerkers van de CHD betrokken, enerzijds om kennis te delen binnen de organisatie en die niet teveel bij alleen de functionaris IB te beleggen. Anderzijds om het tempo van uitvoering te vergroten.

In het plan van aanpak is voorzien een keus te maken over de invulling van de rol van Data Protection Officer. Interne invulling heeft in principe de voorkeur. Of dat voor een organisatie van de omvang van de CHD haalbaar is, ook gezien de eisen die de AVG aan een dergelijke functionaris stelt, is de vraag. Externe inhuur is dan het alternatief, als dat kan samen met collega HDS'en.

Deze breder belegde aanpak zal de komende jaren voortgezet worden. Voor nu is het nog met name gericht op het creëren van beleid en kaders en CHD-brede beheerstechnische maatregelen. Maar wanneer aan de orde en nodig worden mensen uit het primaire proces intensiever bij de PDCA-cyclus en bij de te nemen maatregelen betrokken. Onmisbaar voor begrip en draagvlak. Uiteindelijk is informatiebeveiliging gewoon een (weliswaar wezenlijk) aspect van het primaire proces en kan het niet zo zijn dat zich dat beperkt tot theoretische kaders en overeenkomsten.