Bijlage 2

Informatiebeveiligingsbeleid CIHN

1. Inleiding

Het informatiebeveiligingsbeleid betreft hoofdzakelijk strategische uitgangspunten betreffende de toegang tot en uitwisseling van patiënteninformatie. De tactische en operationele aspecten van informatiebeveiliging zijn te vertalen naar een Informatiebeveiligingsplan.

Informatiebeveiliging heeft betrekking op zowel de geautomatiseerde als niet geautomatiseerde informatie. Het informatiebeveiligingsbeleid van de CIHN i.o. vindt met name zijn oorsprong binnen het project Zorginformatie Nijmegen (ZEGEN). Op 22 september 2005 is het project ZEGEN gestart. Hieraan nemen vier zorgpartners deel: CHN, Huisartsenkring Nijmegen e.o. (toenmalige RHV), Canisius Wilhelmina Ziekenhuis (CWZ), en de regionale apothekers die participeren in de stichting Open Zorg InformatieSysteem Rijk van Nijmegen (OZIS RN).

Het project ZEGEN is door het Nationaal ICT Instituut in de Zorg (NICTIZ) verkozen tot één van de landelijke koplopers voor de invoering van het Elektronische Patiënten Dossier (EPD). Door gebruik te maken van een Elektronisch Patiënten Dossier verbetert de gegevensuitwisseling tussen de diverse zorgaanbieders (huisarts, ziekenhuis en apotheek) en kan het aantal fouten als gevolg van onvolledige of onjuiste informatie sterk verminderen. Kortom: snelle uitwisseling van patiëntengegevens leidt tot:

- Verhoging van de kwaliteit van zorg;
- Kortere doorlooptijden van zorgprocessen;
- Vermindering van administratieve lasten.

Het project ZEGEN behelst twee deelprojecten: het Elektronisch Medicatie Dossier (EMD) en het Elektronisch Waarneem Dossier voor Huisartsen (WDH). De invoering van het elektronisch medicatiedossier maakt het mogelijk dat zorgverleners zicht krijgen op de medicatie die een patiënt gebruikt. Door middel van het elektronisch waarneemdossier kunnen huisartsen tijdens de avond-, nacht en weekeinddiensten op de huisartsenpost van de CIHN inzicht krijgen in de relevante gegevens van de patiënten bij de eigen huisarts.

2. Informatiebeveiliging

Informatiebeveiliging heeft betrekking op het behoud van *vertrouwelijkheid*, *integriteit* en *beschikbaarheid* van (patiënten)informatie binnen de CIHN.

- Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.
- Integriteit: het waarborgen van de correctheid en de volledigheid van informatie en verwerking.
- Beschikbaarheid: het waarborgen dat geautoriseerde gebruikers op het juiste moment toegang hebben tot informatie en middelen.

3. Doel informatiebeveiliging

De Coöperatie voor Integrale Huisartsenzorg Nijmegen e.o. is verantwoordelijk voor de

eerstelijns chronische ketenzorg en de acute huisartsgeneeskundige zorg in avond, nacht en weekend.

Vanuit deze verantwoordelijkheid streeft de CIHN ernaar dat alle informatie die van belang is voor de continuïteit van patiëntenzorg beveiligd wordt, waarbij vertrouwelijkheid, betrouwbaarheid en beschikbaarheid tot op een aanvaardbaar risiconiveau gegarandeerd worden.

Het beleid heeft betrekking op de beveiliging van:

- Persoonsgegevens die verwerkt worden door de CIHN;
- (Patiënten)informatie die ontleend kan worden aan de gegevensverzamelingen van de CIHN of gegevensverzamelingen van derden die de CIHN in haar beheer heeft;
- De (geautomatiseerde) informatiesystemen en andere (geautomatiseerde) informatievoorzieningen van de CIHN.

Dit beleid geldt voor de gehele CIHN en ook voor haar dochtervennootschappen CHN BV en OCE BV.

Het informatiebeveiligingsbeleid is locatieonafhankelijk. Dit betekent dat medewerkers en leden van de CIHN die op een andere locatie dan de huisartsenpost in Nijmegen, Wijchen of Boxmeer werkzaamheden verrichten, het informatiebeveiligingsbeleid dienen te respecteren wanneer zij met informatie of informatievoorzieningen van de CIHN werken.

4. Uitgangspunten informatiebeveiliging

De CIHN kent de volgende **algemene** uitgangspunten voor het informatiebeveiligingsbeleid:

- De fysieke en logistieke beveiliging van de computers en gebouwen van de CIHN is zodanig dat de vertrouwelijkheid, integriteit en continuïteit van de gegevens en gegevensverwerking gewaarborgd zijn.
- Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen mogen geen afbreuk doen aan het bestaande niveau van veiligheid van de geautomatiseerde informatievoorziening.
- Opdrachten verstrekt door de CIHN aan derden worden omgeven met maatregelen, zodat geen inbreuk kan ontstaan op vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening.
- Binnen het personeelsbeleid wordt aandacht geschonken aan het leveren van een bijdrage aan de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening.
- Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van patiënten en medewerkers te waarborgen.
- Logische toegangsbeveiliging zorgt ervoor dat alleen geautoriseerde personen toegang krijgen tot geautomatiseerde systemen, gegevensbestanden en programmatuur binnen de CIHN.
- Het beheer en opslag van gegevens zijn zodanig dat geen informatie verloren kan gaan.
- Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de geautomatiseerde informatievoorziening te waarborgen.

Vanuit de doelstelling van de CIHN zijn de volgende **specifieke** uitgangspunten voor het informatiebeveiligingsbeleid geformuleerd:

- Voor de patiënt en de zorgverlener is een snelle toegang tot zijn patiëntinformatie, met voldoende actuele en relevante informatie van belang voor goede kwaliteit van zorg.
- Patiëntinformatie dient op elke werkplek direct beschikbaar te zijn voor de zorgverlener met een zorgverleningscontact met de patiënt.
- De informatie-uitwisseling tussen zorgverleners van de CIHN en derden verloopt veilig door aansluiting op het LSP en door het gebruik van een eerstelijnsserver met extra beveiligingsmogelijkheden.
- Informatiebeveiliging is de verantwoordelijkheid van iedere medewerker of lid van de CIHN. Iedere medewerker of lid dient zich in het functioneren en het gedrag hiernaar te richten. Door middel van voorlichting wordt dit bewustwordingsproces opgestart, gestimuleerd en gecontinueerd.

5. Taken en verantwoordelijkheden

Het bestuur van de CIHN is eindverantwoordelijk voor de informatiebeveiliging. De directie is verantwoordelijk voor de implementatie van het informatiebeveiligingsbeleid in de organisatie.

Taken en verantwoordelijkheden:
- Het vaststellen en wijzigen van het informatiebeveiligingsbeleid;
- Het toekennen van verantwoordelijkheden;
- Het signaleren van belangrijke wijzigingen in bedreigingen waaraan de bedrijfsinformatie wordt blootgesteld;
- Het bespreken van en toezicht houden op beveiligingsincidenten;
- Het goedkeuren van maatregelen ter verbetering van de informatiebeveiliging.

De directeur heeft het informatiebeveiligingsbeleid ondergebracht in de functie van kwaliteits- en klachtenfunctionaris. De kwaliteits- en klachtenfunctionaris heeft als taak:
- Het implementeren van het informatiebeveiligingsbeleid in de organisatie;
- Het controleren of het informatiebeveiligingsbeleid wordt nageleefd;
- Het nemen van maatregelen ter verbetering van de informatiebeveiliging.

6. Wet- en regelgeving

De CIHN verplicht zich te houden aan alle relevante wetgeving met betrekking tot patiëntgegevens en bedrijfsvoering. Regelmatig zal worden geëvalueerd of nieuwe wetgeving is aangenomen dan wel gewijzigd.
Hieronder wordt een aantal wetten verder uitgediept; de uitwerking hiervan is verwerkt in diverse documenten en procedures.

6.1 Wet gebruik burgerservicenummer in de zorg (Wbsn-z)
Deze wet heeft als doel dat zorgaanbieders zoals de CIHN op grond van het burgerservicenummer kunnen waarborgen dat - in het kader van de zorgverlening - de te verwerken persoonsgegevens op die cliënt betrekking hebben. Alleen met dit unieke nummer kan worden vastgesteld van welke patiënten er gegevens in het landelijke Elektronische Patiënten Dossier zijn en kunnen zijn gegevens worden uitgewisseld.
Vanaf 1 juni 2009 is gebruik van het burgerservicenummer verplicht.

6.2 Goed Beheerd Zorgsysteem (GBZ)
Een Goed Beheerd Zorgsysteem is een zorginformatiesysteem (of een verzameling zorginformatiesystemen) waarmee de zorgaanbieder patiëntgegevens kan uitwisselen met

andere zorgaanbieders. De richtlijn voor een Goed Beheerd Zorgsysteem (GBZ) beschrijft de **algemene eisen** waaraan een systeem minimaal behoort te voldoen op het gebied van beveiliging, performance, communicatie en toegang, opslag en transport van gegevens. Het gaat in hoofdlijnen om de eisen ten aanzien van:

- Connectiviteit: o.a. aansluiting op het LSP via een zorgserviceprovider (ZSP);
- Beveiliging: o.a. in relatie tot gebruik van UZI-passen. Het gebruik van UZI-passen waarborgt dat patiëntengegevens in dossiers en postbussen niet kunnen lekken naar onbetrouwbare bestemmingen en dat patiëntengegevens uit onbetrouwbare bronnen niet terecht kunnen komen in dossiers en postbussen;
- Beschikbaarheid van het systeem;
- Responsetijden;
- Capaciteit;
- Betrouwbaarheid;
- Actualiteit: tijdig aanmelden van wijzigingen in patiëntendossiers;
- Ondersteuning.

Zodra een zorginformatiesysteem voldoet aan bovengenoemde eisen volgens de GBZ kan het zorgsysteem op het LSP worden aangesloten. Het LSP beheert een zogenaamde landelijke verwijsindex, die snel patiëntengegevens opspoort zodra een zorgaanbieder bepaalde informatie over die patiënt opvraagt. Het LSP slaat geen patiëntengegevens op.

6.3 Unieke Zorgverlener Identificatie (UZI) middelen

Een UZI-authenticatiemiddel is een voorwaarde voor veilige elektronische communicatie met de Sectorale Berichten Voorziening in de zorg (SBV-Z) en het LSP. Met een UZI-pas kunnen beroepsbeoefenaars die vallen onder de Wet BIG of die als zorgverlener bij een zorgaanbieder werken hun identiteit aantonen in het elektronische verkeer.
Alleen als zorgverleners een behandelrelatie hebben met een patiënt mogen gegevens worden opgevraagd bij een andere zorgverlener.

De UZI-middelen hebben betrekking op de UZI-passen en het UZI-servercertificaat. De UZI-middelen waarborgen de identificatie en authenticatie van de zorgsystemen en de zorgverleners.

6.4 NEN 7510 informatiebeveiliging in de zorg

NEN 7510 is een algemene norm voor informatiebeveiliging in de zorg. De Inspectie voor de Gezondheidszorg is toezichthouder voor de naleving van deze normering in de zorgsector. De NEN 7510 is meer specifiek uitgewerkt in de NEN 7511 en 7512. Voor de CHN geldt dat zij moet voldoen aan de werkbare criteria volgens de NEN 7511-2.

6.5 Wet op de Computer Criminaliteit (WCC)

De Wet op de Computercriminaliteit is vastgesteld in 2006 en beschrijft de vormen van computercriminaliteit en daarbij behorende straffen. Pc’s en netwerken zijn steeds kwetsbaarder geworden waardoor computercriminaliteit een steeds groter risico vormt. De wet stelt computervredebreuk strafbaar en geeft mogelijkheden voor het opsporen en verzamelen van bewijs tegen verdachten. Onder computervredebreuk wordt onder andere verstaan het vernielen en onbruikbaar maken van netwerken en aftappen van gegevens. De CIHN is zich bewust van deze gevaren en heeft maatregelen genomen om computervredebreuk zoveel mogelijk te voorkomen, bijvoorbeeld door installatie van antivirus-/antispamsoftware, het scheiden van gebruik en beheer van pc’s, het dataverkeer beschermen met beveiligde verbindingen. Deze zaken zijn afgedekt in SLA’s met de belangrijkste partners van de CIHN op het gebied van ICT en patiëntendata. Daarnaast zijn organisatorische maatregelen genomen die verdere risico’s afdekken.

6.6 Wet op Auteursrecht

Alle software die de CIHN onder licentie gebruikt wordt beschermd door auteursrecht. Hiervoor worden licentiekosten betaald. De CIHN werkt niet zonder legitieme licenties.

7. Controle en naleving

Het College Bescherming Persoonsgegevens (CBP) ziet toe op de naleving van de Wet Bescherming Persoonsgegevens. Deze wet is ook van toepassing op het landelijk EPD. De Inspectie voor de Gezondheidszorg (IGZ) richt zich op het naleven van regels rondom verantwoorde zorg.

Zoals eerder beschreven is het CIHN-bestuur eindverantwoordelijk voor de informatiebeveiliging binnen de CIHN. Handhaving en evaluatie van dit beleid wordt gedelegeerd aan de CIHN-directeur.

De uitvoering van het werkplan ten behoeve van de informatiebeveiliging wordt ieder jaar in overeenstemming met de planning- en controlecyclus door de kwaliteits -en klachtenfunctionaris geëvalueerd.

8. Documentatie

Het informatiebeveiligingsbeleid is verder uit te werken in een informatiebeveiligingsplan en een middelenmatrix. Daarnaast is het vast te leggen in diverse procedures die in een handboek Kwaliteit zijn op te nemen.