

## Gezamenlijke verantwoordelijkheid

Het Parelsnoer Initiatief (PSI) verzamelt klinische gegevens en lichaamsmaterialen van patiënten ten behoeve van wetenschappelijk onderzoek. Met deze informatie moet nauwgezet worden omgegaan. Zorgvuldig handelen is essentieel om tot goede onderzoeksresultaten te komen en leidt tot vertrouwen bij patiënten die hun gegevens en lichaamsmateriaal beschikbaar stellen. Bovendien schrijft de privacywetgeving zorgvuldigheid voor. Daarom heeft de directie van PSI eind 2008 een informatiebeveiligingsbeleid voor de organisatie vastgesteld.

Het informatiebeveiligingsbeleid heeft tot doel alle gegevens en informatiestromen binnen PSI optimaal te krijgen en te houden voor wat betreft:

- de toegankelijkheid van de gegevens (beschikbaarheid);
- de kwaliteit en eenduidigheid van de gegevens (integriteit);
- het gebruik van gepseudonimiseerde gegevens voor wetenschappelijk onderzoek en niet voor andere doeleinden (vertrouwelijkheid).

Om dit te bereiken zijn tal van maatregelen noodzakelijk, zowel op technisch, organisatorisch als procedureel vlak. Deze maatregelen moeten samen een geheel vormen en door de hele organisatie gedragen en nageleefd worden.

De directie van PSI hecht groot belang aan informatiebeveiliging. Een information security officer en een werkgroep Informatiebeveiliging geven richting aan en houden toezicht op de feitelijke uitwerking van het informatiebeveiligingsbeleid in praktische werkwijzen. Het is essentieel dat alle betrokkenen doordrongen zijn van het belang van informatiebeveiliging. Ze moeten op de hoogte zijn van hun verantwoordelijkheden en zich ervan bewust zijn dat zij zelf een bijdrage kunnen en moeten leveren. Beveiliging moet 'leven' en niet alleen op papier zijn vastgelegd.

### Kernpunten informatiebeveiliging

De werkgroep Informatiebeveiliging heeft de relevante wetten en normen, waaronder de norm voor informatiebeveiliging in de zorg NEN7510, vertaald naar

de situatie binnen PSI. Het informatiebeveiligingsbeleid dat daaruit is voortgekomen, heeft als kernpunten:

- informatiebeveiliging is de verantwoordelijkheid van de hele organisatie, dus ook van het management;
- informatiebeveiliging is een serieuze zaak en stelt eisen aan alle medewerkers die met gegevens werken binnen PSI en binnen de onderdelen van de UMC's betrokken bij PSI;
- waarborging van de privacy van patiënten is een essentiële voorwaarde bij het ter beschikking stellen van gegevens.

In het beleidsdocument staat globaal welke maatregelen genomen moeten worden om de veiligheid te waarborgen. Deze bestrijken het hele gebied van beleid tot operationele zaken, zoals bijvoorbeeld: risicoanalyse voor processen en gegevens, voorlichting aan en afspraken met medewerkers, adequate back-up voorzieningen, maatregelen tegen kwaadaardige software en goede toegangsbeveiliging van de systemen. Deze globale maatregelen worden in detail uitgewerkt binnen de procedures en werkwijzen van PSI. Dit betekent dat het beleid vertaald wordt naar de architectuur en ontwerpdocumentatie van de verschillende systemen en processen. Zorgvuldig omgaan met informatie is immers een onlosmakelijk onderdeel van de dagelijkse praktijk.

### Reikwijdte

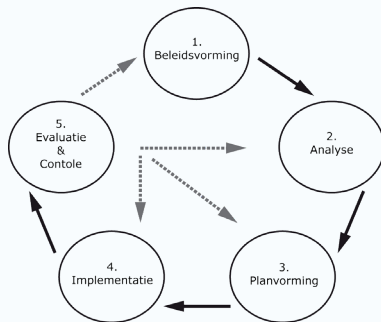
Het Informatiebeveiligingsbeleid geldt voor de gehele organisatie van PSI, dat wil zeggen: voor de centrale organisatie

en voor de bij PSI betrokken onderdelen van de UMC's. Dit vraagt om een goede afstemming met de UMC's. Hierbij is het reeds bestaande, reguliere overleg tussen de UMC's op het gebied van informatiebeveiliging (de Special Interest Group Informatiebeveiliging) het eerste aanspreekpunt.

### Informatiebeveiliging en kwaliteit

Informatiebeveiliging is een belangrijk aspect van de algehele kwaliteitszorg binnen PSI. Een goede inpassing in het kwaliteitssysteem is daarom onontbeerlijk. De maatregelen die voortkomen uit het informatiebeveiligingsbeleid moeten zodanig geborgd zijn in het kwaliteitssysteem, dat het beveiligingsniveau gehandhaafd blijft. Om dit te bereiken en de actualiteit van het informatiebeveiligingsbeleid te waarborgen, wordt een beleidscyclus gehanteerd. Deze omvat vijf stappen:

1. vaststellen van het informatiebeveiligingsbeleid;
2. analyse van de bestaande situatie, zowel op centraal als decentraal niveau, om inzicht te krijgen in de kwaliteit van bestaande beveiligingsmaatregelen en risico's;
3. opstellen van een informatiebeveiligingsplan, dat wordt vastgesteld door de directie van PSI;
4. implementatie van aanvullende beveiligingsmaatregelen aan de hand van het informatiebeveiligingsplan;
5. periodieke controle of de gewenste effecten zijn bereikt. Op basis daarvan kan de cyclus opnieuw worden doorlopen.



Figuur: Beleidscyclus informatiebeveiliging

Net als bij kwaliteitszorg, vereist informatiebeveiliging dat de organisatie zich aan bepaalde richtlijnen houdt. Om te beoordelen of die richtlijnen duidelijk beschreven zijn en zijn ingebed in de dagelijkse gang van zaken, wordt in het project een werkwijze opgezet waarin periodieke toetsing (via interne en/of externe audits) plaatsvindt.

## Het Parelsnoer Initiatief

Het Parelsnoer Initiatief realiseert een unieke samenwerking tussen de acht universitair medische centra. Het Parelsnoer Initiatief, opgericht in 2007 door de Nederlandse Federatie van Universitair Medische Centra (NFU), verzamelt op interuniversitair niveau klinische data en biomaterialen.

Door het bundelen van deze gegevens en materialen kan de wetenschap zich ontwikkelen, wordt de patiënt nog beter behandeld en kan nieuwe productontwikkeling plaatsvinden. Dit versterkt de economische positie van het biomedisch onderzoek in Nederland.

Het project richt zich in eerste instantie op negen ziektebeelden (genaamd parels). In de toekomst kunnen de activiteiten van het Parelsnoer Initiatief uitgebreid worden naar andere ziektebeelden.

Voor meer info kunt u terecht op de website, [www.parelsnoer.org](http://www.parelsnoer.org) of kunt u contact opnemen met het Parelsnoer Initiatief via [info@parelsnoer.org](mailto:info@parelsnoer.org).