**Privacy: verboden terrein
**

*Een onderzoek naar het privacy beleid binnen organisatie SCAL en de nieuwe algemene Europese verordening omtrent beschermen persoonsgegevens.*



Student: Veronique Ras
Studentnummer: 1059707
Opleiding: Sociaal Juridische Dienstverlening
Instituut: Hogeschool Leiden
Collegejaar: 6
Inleverdatum: 01-09-2016
Opdrachtgever: SCAL
Contactpersonen: G. De Ruijter
Afstudeerbegeleider: M. Kroft
Afstudeercoördinator: E. Mudde

**Samenvatting**Per 01 januari 2018 zal de verordening betreffende de bescherming van individuen in verband met het verwerken van persoonsgegevens en het vrije verkeer van die gegevens volledig geïmplementeerd zijn in de nationale wetgeving van Nederland. De verordening, ook wel algemene verordening gegevensbescherming, is deels al van kracht op het gebied van datalekken. De overige relevante onderwerpen voor opdrachtgever SCAL zijn; de verscherping van het toestemmingsvereiste, informatievoorziening naar de cliënt toe, toename van administratieve handelingen en het invoeren van risico analyses om het privacy beleid binnen de organisatie te toetsen. Tevens zal naar alle waarschijnlijkheid de verplichting om een functionaris voor privacy bescherming aan te stellen ook voor SCAL gelden.

Er is onderzoek gedaan naar het huidige privacy beleid binnen SCAL gedurende het uitvoeren van een bloedonderzoek. Er is bekeken op welke wijze het beleid is vastgelegd in protocollen en handleidingen. Daarnaast is onderzocht of dit geschreven beleid overeen komt met de wet en regelgeving vastgelegd in de algemene verordening gegevensbescherming. Om vervolgens te onderzoeken op welke wijze de praktijkvoering is bij de weg die de persoonsgegevens van de cliënt afleggen als er een bloedonderzoek in werking wordt gezet.
De conclusie die gesteld kan worden naar aanleiding van bovenstaande onderzoekswegen is dat het huidige privacy beleid van opdrachtgever SCAL (nog) niet voldoet aan de vereisten opgenomen in de algemene verordening gegevensbescherming. Met name het beleid omtrent datalekken dient spoedig ontwikkelt te worden aangezien de wet en regelgeving op dit gebied al van kracht is sinds 01 januari 2016. Voor alle overige aanbevelingen geldt nog een overgangstermijn tot 01 januari 2018.

De overige aanbevelingen zijn; het toestemmingsvereiste in het beleid binnen de organisatie op te nemen, informatievoorziening richting de cliënt verbeteren, een functionaris voor privacy bescherming aan te stellen en het nieuwe privacy beleid levend te maken, en dan met name bij het uitvoerend personeel. Tevens bestaat de mogelijkheid voor SCAL om een advies te vragen middels een beoordeling van het privacy beleid door Autoriteit Persoonsgegevens.

Inhoudsopgave

1.Inleiding blz.4 t/m 6
1.1 Aanleiding en achtergrond blz.4 1.2Probleemanalyse en afbakening van het probleem blz.5
1.3 Doelstelling en vraagstelling blz.5
1.4 Praktische en theoretische relevantie blz.6

2. Aanpak van het onderzoek blz.7 t/m 8
2.1 Verantwoording van gekozen methodes blz.7 t/m 8

3 Juridisch kader en toepassing op SCAL blz.9 t/m 31
3.1 Juridisch kader blz.9
3.1.1 Huidige Europese & Nationale wet- en regelgeving blz.9 t/m 15
3.1.2 Nieuwe Europese richtlijn blz.15 t/m 21
3.1.3 Toepassing huidige wet- en regelgeving en de nieuwe algemene verordening gegevensbescherming op SCAL blz.22 t/m 24
3.2 Documentenanalyse blz.25 t/m 29
3.3. Conclusie juridische & documenten analyse blz.30 t/m 31

4. Praktijkuitvoering blz.32 t/m 42
4.1 Interviews leidinggevenden blz.32 t/m 33
4.2 Scan uitvoerend personeel blz. 34 t/m 40
4.3 Conclusie praktijkvoering blz.41 t/m 42

5. Aanbevelingen blz.43 t/m 44

Literatuurlijst blz. 46 t/m 47

Bijlagen blz. 48 t/m 94
1. Relevante artikelen, schending, maatregelen Autoriteit Persoonsgegevens blz. 48 t/m 49
2. Privacy iconen blz. 49
3A. Aannemen van een aanvraag blz. 49 t/m 50
3B. Baliewerkzaamheden blz. 51
3C. Zoeken in Vecozo programma blz. 51
3D. Rapportage blz. 52 t/m 53
3E. Archiveren en vernietigen van documenten
 en archivering van aanvraagformulieren blz. 53 t/m 54
3F. Bewaartermijnen documenten blz. 55
3G. Acties na overblijven van een buis en acties na het missen van een buis blz. 55 t/m 56
4. Inleidende toelichting interview blz. 57
5A. Interviews leidinggevenden blz. 58 t/m 71
5B. Scan uitvoerend personeel blz. 72 t/m 92
6. Beroepsproduct (advies) blz. 93 t/m 94

**Hoofdstuk 1. Inleiding**

Op 19 januari 2016 heeft de Europese Raad en het Europees Parlement het voorstel van de Europese Commissie met betrekking tot gegevensbescherming aangenomen. Het betreft hier een verordening betreffende de bescherming van individuen in verband met het verwerken van persoonsgegevens en het vrije verkeer van die gegevens. Hierna te noemen Algemene verordening gegevensbescherming. Het zal nog enkele maanden duren voordat de verordening officieel wordt aangenomen middels een stemming in de Europese Raad en het Europees Parlement. Pas na bekendmaking van de algemene verordening gegevensbescherming in het publicatieblad van de Europese Unie zal deze in werking treden. Er geldt een overgangstermijn van 2 jaren. Dit betekent dat de Europese lidstaten deze tijd mogen benutten om de internationale wetgeving te verwerken in hun eigen nationale wetgeving. Nederland is al begonnen met voorbereidingen op implementatie van de verordening. Deze nieuwe wetgeving zorgt voor wijzigingen in onder andere de Wet bescherming persoonsgegevens (Wbp).
Vanwege de complexiteit van het vraagstuk over het privacy beleid binnen de gezondheidszorg en naar aanleiding van deze nieuwe wetgeving, heeft opdrachtgever SCAL mij verzocht onderzoek te doen naar welke aanpassingen deze Algemene verordening gegevensbescherming zal vergen voor haar organisatie.

1.1 Aanleiding en achtergrond
Op donderdag 17 april 2014 wordt er een documentaire van programma Zembla uitgezonden[[1]](#footnote-1) over het delen van medische gegevens door medische instanties met zorgverzekeraars. Naar aanleiding van een groot schandaal in Engeland, waarbij medische instanties volledige medische dossiers verkochten aan zorgverzekeraars, werd de vraag gesteld hoe het in Nederland gesteld is met de ‘medische’ privacy van burgers. Op dat moment was er in de Nationale en Europese politiek al volop discussie gaande over een nieuwe algemene verordening omtrent privacy. De verordening zal de huidige Europese privacy richtlijn[[2]](#footnote-2) vervangen en moet zorgen voor een meer uniform beleid binnen de Europese Unie. Dit zal kunnen betekenen dat organisaties zoals SCAL flinke aanpassingen moeten doorvoeren in hun privacy beleid, om sancties van Autoriteit Persoonsgegevens (hierna AP te noemen) te voorkomen.

Omdat SCAL zich bezig houdt met diagnostisch onderzoek en hiermee veel privacygevoelig informatie verzamelt, deelt en archiveert zal de opdrachtgever zich moeten voorbereiden op de invoering van de algemene verordening gegevensbescherming. Om het onderzoek overzichtelijk te houden zal de onderzoeker zich richten op één van de meest uitgevoerde diagnostische onderzoeken; bloedonderzoek. Dit onderzoek wordt vaak in opdracht van medische specialisten en ziekenhuizen gedaan, maar het is ook mogelijk om onderzoek te laten doen zonder tussenkomst van een derde partij. Opdrachtgever SCAL is eindverantwoordelijk voor een goede verloop van het diagnostisch onderzoek dat bestaat uit meerdere handelingen op afzonderlijke afdelingen. Juist omdat tijdens het bloedonderzoek op verschillende afdelingen (gevoelige) persoonsgegevens worden verwerkt was het van belang hier op in te zoomen.

1.2 Probleemanalyse en afbakening van het probleemMomenteel is voor de organisatie het begrip privacy een complex vraagstuk waarbij gebrek is aan overzicht. Veel aandacht is er voor de beveiliging van de computersystemen, waar SCAL al heel druk mee is. Maar wat wordt er verwacht op het gebied van het beleid rondom cliëntencontact? Wat moet er bijvoorbeeld met de cliënt worden besproken en welke gegevens mogen er worden gevraagd en waar moeten deze gegevens dan worden opgeslagen? De antwoorden op deze vragen zijn met de invoering van de Algemene verordening gegevensbescherming wellicht anders dan met de huidige wet- en regelgeving. Wat deze wijzigingen en aanvullingen exact betekenen voor organisaties in de gezondheidssector is niet duidelijk voor SCAL.
Het is zaak voor SCAL om zo spoedig mogelijk helder te hebben welke eventuele aanpassingen er specifiek voor de werkprocessen tijdens het bloedonderzoek gelden als het om privacy beleid gaat. De hoeveelheid privacy gevoelige informatie waarmee SCAL dagelijks te maken krijgt brengt een grote verantwoordelijkheid met zich mee. De toename van maatregelen die uit deze verantwoordelijkheid voortvloeien dwingt de opdrachtgever serieuze stappen te ondernemen haar privacy beleid onder de loep te nemen en zo nodig te verbeteren. 1.3 Doelstelling en vraagstellingDe opdrachtgever wilt een zorgvuldig privacy beleid hanteren dat voldoet aan de algemene verordening gegevensbescherming. Daarom is belangrijk om weet te hebben van wat de algemene verordening gegevensbescherming voor de nationale wet- en regelgeving en beleid op het gebied van privacy specifiek zullen betekenen. Daarnaast is het van belang om kennis te hebben van hoe het huidige privacy beleid van de organisatie op papier zijn uitwerking in de praktijk heeft. Welke aanpassingen dienen, op basis van de nieuwe wetgeving, te worden ingevoerd in deze organisatie en wat betekent dit voor het huidige privacy beleid binnen SCAL?

Op grond van de probleemstelling en het doel dat men wilt bereiken met dit onderzoek is de volgende centrale vraag geformuleerd:
**“In hoeverre voldoet het privacy beleid van SCAL aan de algemene verordening gegevensbescherming?”**
Om bovenstaande vraag te kunnen beantwoorden is het van belang om aan de hand van een aantal deelvragen informatie te verschaffen:

**1.** Aan welke eisen dient het privacy beleid te voldoen op basis van de huidige wet en regelgeving?

**2.** Aan welke eisen dient het privacy beleid te voldoen in het kader van de algemene verordening gegevensbescherming?

**3.** Hoe is de privacy van de cliënten van SCAL gewaarborgd in het huidige beleid van SCAL tijdens het uitvoeren van bloedonderzoek?

**4.** Welke wijzigingen dient SCAL in haar werkprocessen, bij het uitvoeren van bloedonderzoek, door te voeren om te voldoen aan de algemene verordening gegevensbescherming?

1.4 Praktische en theoretische relevantieSCAL heeft behoefte aan duidelijke juridische kaders waarmee zij voorbereidingen kunnen treffen voor de invoering van de algemene verordening gegevensbescherming.
Opdrachtgever SCAL heeft verzocht om het onderzoek te richten op een veelvoorkomend onderzoek dat uitgevoerd wordt door haar werknemers, namelijk bloedonderzoek. De opdrachtgever zal door de uitkomsten van dit onderzoek vervolgens verder kunnen uitzoeken hoe zij het privacy beleid ook bij de andere diagnostische onderzoeken kan toepassen. De verschillende handelingen op afzonderlijke afdelingen binnen SCAL, die betrokken zijn bij (de verwerking) bloedonderzoek, zullen fungeren als voorbeeld, waar men verder op kan voortborduren.
Het product dat voortvloeit uit het gedane onderzoek is in de vorm van een advies. Dit advies gaat in op de eventuele knelpunten in het privacy beleid bij SCAL en hier mogelijke oplossingen voor aandragen. Het advies is de voorbereiding op de komst van de algemene verordening gegevensbescherming.

**Hoofdstuk 2 Aanpak van het onderzoek**
Gedurende het onderzoek is gebruik gemaakt van twee onderzoeksmethoden; het afnemen van interviews en uitgebreide documentanalyse. In het volgende hoofdstuk wordt aangegeven welke methode wordt gebruikt bij de beantwoording van de verschillende deelvragen.

2.1 Verantwoording van gekozen methodes **Documentenanalyse**Omdat er een algemene verordening gegevensbescherming klaar ligt ter implementatie voor de Nederlandse wetgeving is documentanalyse zeer belangrijk. Naast analyse van de nieuwe verordening zijn ook alle protocollen en handleidingen omtrent verwerken persoonsgegevens van opdrachtgever SCAL bestudeerd. Tevens zijn ook andere betrouwbare en relevante bronnen geraadpleegd zoals jurisprudentie, nieuwsberichten en publicaties van de overheid.
Dit onderdeel van het onderzoek is van belang om in beeld te krijgen wat de huidige situatie is op het gebied van wet- en regelgeving voor bescherming van persoonsgegevens. Vervolgens zijn er conclusies getrokken uit het raadplegen van het geschreven beleid van SCAL. Voldoet dit geschreven beleid aan de huidige wet- en regelgeving? Aansluitend is bestudering van de nieuw ingevoerde algemene verordening gegevensbescherming noodzakelijk geweest om een advies te kunnen schrijven over aanpassingen die SCAL zal moeten doen ter implementatie van deze nieuwe verordening.

Gedurende het onderzoek is er een verzameling ontstaan van relevante documenten. Deze zijn gelabeld opgeslagen op de computer en gesorteerd op soort document. Op deze manier is het document gemakkelijk terug te vinden en te gebruiken als informatiebron.
Bij grote documenten zijn de relevante teksten in het stuk geselecteerd en aangegeven per kleur.
Tevens is bij gebruik van bronvermelding in de gaten gehouden of dit een betrouwbare bron betreft. De betrouwbaarheid is goed te herkennen op het moment dat meerdere onafhankelijke stukken dezelfde informatie geven. Documentanalyse heeft volledig antwoord gegeven op onderstaande deelvragen:
**1.** Aan welke eisen dient het privacy beleid te voldoen op basis van de huidige wet en regelgeving?
**2.** Aan welke eisen dient het privacy beleid te voldoen in het kader van de algemene verordening gegevensbescherming?
Onderstaande deelvragen zijn deels beantwoord door documentanalyse:
**3.** Hoe is de privacy van de cliënten van SCAL gewaarborgd in het huidige beleid bij het uitvoeren van bloedonderzoek?
**4.** Welke wijzigingen dient SCAL in haar werkprocessen, bij het uitvoeren van bloedonderzoek, door te voeren om te voldoen aan de nieuwe wet en regelgeving op het gebied van privacy?

Aansluitend was het nodig om interviews af te nemen bij betrokken personeel van SCAL om tevens de uitvoering in de praktijk vast te stellen.
 **Interviews**Middels het afnemen van interviews wordt duidelijk in beeld gebracht hoe het geschreven beleid van SCAL zijn uitwerking in de praktijk heeft. De interviews zijn afgenomen bij de leidinggevenden en uitvoerend personeel van de afdelingen die doorlopen worden als een cliënt bloedonderzoek laat uitvoeren. Het is zaak onderscheidt te maken tussen leidinggevenden en uitvoerend personeel dat onder de verantwoordelijkheid van deze leidinggevenden staan. De leidinggevenden worden geïnterviewd over het beleid en de werkprocessen. Mede omdat zij volgens de wetgeving geacht worden hiervan op de hoogte te zijn en dit ook over dienen te dragen aan het uitvoerend personeel. Het uitvoerend personeel wordt geïnterviewd over het beleid in de praktijk, hoe gaan zij daadwerkelijk te werk en op welke wijze houden zij zich aan het geschreven beleid rondom privacy.
Het proces van bloedonderzoek doorloopt drie verschillende afdelingen: receptie, medical services en laboratorium. Deze afdelingen houden zich dagelijks bezig met het verzamelen, verspreiden en archiveren van privacy gevoelige informatie.
De gestructureerde interviews met de leidinggevenden geven een duidelijk beeld weer van de uitvoering van het privacy beleid door hen binnen de organisatie. Dit was nodig omdat de uitgevoerde documentenanalyse voor veel vragen zorgde die de leidinggevende geacht hoort te weten.

Gekozen is voor de gestructureerde interviewmethode omdat de onderzoeker voornamelijk wilde vaststellen wat de kennis, van de leidinggevende is op het gebied van privacy en hoe zij in de praktijk uitvoering geven aan het privacy beleid. Door half open interviews wordt er ruimte geboden aan de geïnterviewden om hun visie en ervaringen naar voren te brengen zodat de onderzoeker zicht krijgt op de problematiek.
Per afdeling is één leidinggevende geïnterviewd, wat neer komt op drie afgenomen interviews. Het afnemen van interviews heeft onderstaande deelvragen, in combinatie met documentanalyse, doen beantwoorden:
**3.** Hoe is de privacy van de cliënten van SCAL gewaarborgd in het huidige beleid bij het uitvoeren van bloedonderzoek?
**4.** Welke wijzigingen dient SCAL in haar werkprocessen, bij het uitvoeren van bloedonderzoek, door te voeren om te voldoen aan de algemene verordening gegevensbescherming?Ter voorbereiding van de afgenomen interviews is een vragenlijst gecreëerd aangepast op de betreffende handelingen die uitgevoerd worden op de afdeling waar de betreffende leidinggevende werkt. Deze handelingen zijn gericht op het doen van bloedonderzoek of de verwerking van de resultaten daarvan. Alvorens het interview zijn een aantal begrippen kort uitgelegd middels een A4, *zie bijlage 4*.
Voorafgaand aan het afnemen van de interviews is de vooraf opgestelde vragenlijst uitgeprobeerd in een pilot waarbij zes mensen zijn geïnterviewd los van de organisatie. Dit om de manier van vragen stellen te verbeteren en aan te scherpen.
Om de betrouwbaarheid te waarborgen is elk interview opgenomen met audioapparatuur. Vervolgens zijn de interviews volledig uitgeschreven en gelabeld. De labels vertegenwoordigen de belangrijke uitspraken en overeenkomsten en/of tegenstellingen met andere geïnterviewden.

Door het uitvoeren van deze diepte interviews is een scan opgesteld waarbij gecontroleerd is of voldaan wordt aan de wettelijk regels omtrent privacy beleid.

**Scan**De scan, die opgesteld is aan de hand van de diepte interviews met de leidinggevenden, is bij meerdere medewerkers van de verschillende afdelingen afgenomen. De scan bestaat uit gestructureerde half open vragen en is toegepast bij zes medewerkers van de relevante afdelingen. Met daarnaast drie interviews met de leidinggevenden van de betreffende afdelingen. Zij waren op dat moment betrokken bij een werkproces voor het uitvoeren van een bloedonderzoek. Op deze wijze is heel concreet te concluderen waar wel en waar niet aan voldaan wordt binnen de organisatie als het gaat om bescherming van persoonsgegevens.
De resultaten van de uitgevoerde scan is schematisch weergeven en terug te lezen in hoofdstuk 4.1.

**Hoofdstuk 3 Sociaal juridisch kader**3.1 Juridisch kaderOpdrachtgever SCAL valt met betrekking tot gegevensverwerking voornamelijk onder de werkingssfeer van de Wet bescherming persoonsgegevens (Wbp). Dit omdat SCAL op grote schaal persoonsgegevens verwerkt bij het uitvoeren van een bloedonderzoek. De Wbp, nationale wetgeving van Nederland, is een implementatie van de Europese privacyrichtlijn die op 24 oktober 1995 in werking is getreden. Naast de Wbp is ook de overeenkomst inzake geneeskundige behandeling (WGBO) en de wet op de beroepen in de individuele gezondheidszorg (BIG) van belang voor de privacy van de cliënten van SCAL (betrokkenen). De WGBO en BIG zijn bijzondere regelingen in verhouding tot de Wbp. Dit houdt in dat waar de Wbp wetgeving is in algemene zin, de WGBO en BIG specifieke regels aangeven met betrekking tot privacy voor een bepaalde groep. Namelijk degenen die een geneeskundige behandelingsovereenkomst zijn aangegaan.
Omdat opdrachtgever SCAL bijna altijd in opdracht van ziekenhuizen, specialisten en huisartsen werkt valt zij onder Artikel 446 lid 1 jo. Lid 2 WGBO. De constatering is dat ook al handelt SCAL in opdracht van een andere medische instantie er alsnog sprake kan zijn van een geneeskundige behandelingsovereenkomst. Onder andere wordt specifiek het verrichten van onderzoek genoemd. Dit betreft ook bloedonderzoek ten behoeve van het stellen van bijvoorbeeld een diagnose. Tegelijkertijd vloeit uit deze overeenkomst de verplichting van goed hulpverlenersschap. Dit houdt in dat de verantwoordelijke de regels naar de wet WGBO uitvoert. Daarnaast dient de wet in algemene zin, de Wbp, ten alle tijden worden nageleefd.
Tevens dienen de verpleegkundigen die alvorens het bloedonderzoek bij cliënt bloed prikken geregistreerd te staan in het BIG register, aldus Artikel 3 lid 1 BIG. Het doel van deze wetgeving is dat de beroepstitel hiermee beschermd blijft. Niet iedereen kan zich zomaar arts of verpleegkundige noemen. Alleen zij die geregistreerd staan in het register mogen voorbehouden handelingen uitvoeren. Dit zijn medische handelingen die onaanvaardbare risico’s voor de gezondheid van de cliënt met zich meebrengt als iemand zonder deskundigheid deze uitvoert. Het feit dat deze werknemers geregistreerd staan brengt met zich mee dat zij ter verantwoording kunnen worden geroepen bij het tuchtrecht.

In dit hoofdstuk wordt uitgelegd wat deze nationale wet- en regelgeving inhoudt en wat dit betekent voor de huidige situatie bij SCAL. Vervolgens wordt de toekomst bekeken aan de hand van nieuwe Europese wet- en regelgeving omtrent bescherming persoonsgegevens.

3.1.1 Huidige Europese en nationale wet- en regelgeving

De Europese Unie is opgericht om mogelijkheid te bieden tot een gezamenlijk beleid van lidstaten met betrekking tot bepaalde onderwerpen. De onderwerpen (toepassingsgebieden) waar de Europese Unie zich mee bezig houdt zijn vastgelegd in Europese verdragen. Per toepassingsgebied is aangegeven wat de bevoegdheden van de EU en de lidstaten zijn. Er zijn een aantal mogelijkheden:
1. De EU maakt het beleid en dat moet door alle lidstaten worden opgevolgd
2. De EU heeft geen bevoegdheid om beleid te maken
3. De EU ondersteund de lidstaten bij het maken van beleid
4. De EU en lidstaten delen de bevoegdheid om beleid te maken
De Europese Unie heeft gedeelde bevoegdheid met de lidstaten als het o.a. gaat om het toepassingsgebied ruimte van vrijheid, veiligheid en recht (valt dus onder 4) [[3]](#footnote-3). Het privacy recht dat in Nederland voornamelijk is geregeld via de Wbp valt onder te brengen in dit toepassingsgebied. Tevens wordt het privacy recht van burgers expliciet genoemd in artikel 16 VWEU[[4]](#footnote-4). Hierin beschrijft men dat, om ieders recht op bescherming persoonsgegevens te waarborgen, het Europees Parlement en de Raad voorschriften ontwikkelen die nageleefd moeten worden door lidstaten. Op de naleving van deze voorschriften wordt toezicht gehouden door onafhankelijke autoriteiten. De onafhankelijke nationale autoriteit van Nederland is de Autoriteit Persoonsgegevens (AP).

***Artikel 29-werkgroep***
Op Europees niveau is een werkgroep ingesteld. Dit om een gemeenschappelijk beleid met alle lidstaten van de EU te bereiken. De Artikel 29-werkgroep[[5]](#footnote-5) is een onafhankelijk orgaan dat adviseert en overlegt over totstandkoming van Europees beleid voor bescherming van persoonsgegevens. De werkgroep bestaat uit nationale privacy toezichthouders van lidstaten en de European Data Potection (Hierna te noemen EDPS). Nederlands jurist Peter Hustinx is hoofd van deze organisatie. EDPS houdt toezicht op verwerking van persoonsgegevens bij instellingen van de Europese Unie.
De belangrijkste taak van de werkgroep is het bevorderen van een uniforme toepassing van de privacyrichtlijn. Daarnaast doen ze onderzoek waaruit nationaal beleid ontstaat. Tevens geven ze advies aan de Europese Commissie over het volgende:
- Nieuwe Europese privacy wet- en regelgeving en voorstellen voor de bescherming van persoonsgegevens
- Bescherming van persoonsgegevens in de Europese Unie
- Gedragscodes op Europees niveau
- Beschermingsniveau van derde landen

***(Bijzondere) persoonsgegevens***
De Wbp geeft opdrachtgever SCAL veel wettelijke kaders waarbinnen gewerkt dient te worden. Zo wordt er in Artikel 1 sub a Wbp beschreven wat er verstaan wordt onder een persoonsgegeven.

Als gegevens direct of indirect informatie bevatten over een persoon die hem/haar identificeerbaar maakt is er sprake van een persoonsgegeven. Dit kunnen sec de naam, adres, foto, gironummer enzovoorts zijn. Maar ook als een gegeven indirect herleidt kan worden naar de betreffende persoon valt het onder de noemer persoonsgegevens. Indirecte gegevens zijn bijvoorbeeld de winst van een eenmanszaak, kenteken van een auto of een luchtfoto van een huis.

Daarnaast maakt men onderscheidt in persoonsgegevens en bijzondere persoonsgegevens. Onder bijzondere persoonsgegevens wordt verstaan: ras, politieke overtuiging, godsdienst, seksuele voorkeur, gezondheid, strafrechtelijke persoonsgegevens en lidmaatschap van een vakvereniging. Het is verboden om deze bijzondere gegevens te verwerken tenzij voldaan wordt aan één van de genoemde uitzonderingen in Artikelen 17 t/m 22 Wbp. Een relevante uitzondering voor opdrachtgever SCAL staat genoemd in Artikel 21 Wbp.
Artikel 21 lid 3 Wbp zegt hier het volgende over: “*3. Het verbod om andere persoonsgegevens als bedoeld in Artikel 16 te verwerken, is niet van toepassing voor zover dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid als bedoeld in het eerste lid, onder A, met het oog op een goede behandeling of verzorging van de betrokkene.”* Het derde lid geeft aan dat er specifieke situaties kunnen zijn waar in het belang van een goede geneeskundige behandeling en verzorging van cliënten in aanvulling op gezondheidsgegevens andere gevoelige persoonsgegevens moeten worden verwerkt. Ook het gegeven ras en seksuele voorkeur kan soms een belangrijk gegeven zijn bij een diagnosestelling. Het kan dan zijn dat een bepaald gegeven zoals ras of seksuele voorkeur hierdoor een medisch karakter krijgt. Om die reden kan het noodzakelijk zijn deze gegevens met het oog op een goede geneeskundige behandeling te verwerken.

***Verwerking persoonsgegevens***
Artikel 1 sub b Wbp beschrijft dat indien één of meerdere van de volgende handelingen worden verricht, er sprake is van verwerking van persoonsgegevens:
– Verzamelen, vastleggen, ordenen
– Bewaren, bijwerken, wijzigen
– Opvragen, raadplegen, gebruiken
– Verstrekken door middel van doorzenden
– Samenbrengen en met elkaar in verband brengen
– Afschermen, uitwisselen, of vernietigen
– Verspreiding of enige vorm van terbeschikkingstelling
Deze handelingen dienen te worden uitgevoerd naar de regel van de Wbp en WGBO.

Van de verantwoordelijke[[6]](#footnote-6) wordt verwacht maatregelen te treffen zodat persoonsgegevens op een nauwkeurige en juiste manier verwerkt worden.[[7]](#footnote-7) Daarnaast dient de verantwoordelijke toe te zien op de getroffen maatregelen vanwege zijn zogenoemde zorgplicht[[8]](#footnote-8).
Tevens geeft de wetgeving aan dat er tijdens gegevensverwerking een aantal uitgangspunten een belangrijke rol dienen te spelen:
– Artikel 6 Wbp heeft het over terughoudendheid
– In de memorie van toelichting[[9]](#footnote-9) van de Wbp wordt meerdere keren openheid genoemd. Hiermee wordt bedoeld dat iedere cliënt in de gelegenheid moet zijn om na te kunnen gaan waar zijn gegevens worden verwerkt en op welke wijze.
– Artikel 7 jo. 9 Wbp noemt doelbinding . Hiermee wordt bedoeld dat persoonsgegevens alleen voor welbepaalde, nadrukkelijk omschreven en gerechtvaardigde doeleinden mag worden verzamelt. Deze doelen zijn vooraf besproken met betrokkene. Artikel 448 lid 2 sub a WGBO benoemt tevens de verplichting van doelbinding.
– Artikel 13 Wbp noemt extra bescherming. Hiermee wordt bedoelt dat de organisatie, waar betrokkene zijn persoonsgegevens mee deelt, verplicht is passende technische en organisatorische maatregelen te nemen omtrent beveiliging van deze gegevens. De beveiliging dient gericht te zijn op voorkoming van verlies of enige vorm van onrechtmatige verwerking of op het onnodig verzamelen van cliëntgegevens.

Daarnaast geeft Artikel 8 Wbp een aantal relevante criteria voor het verwerken van persoonsgegevens voor opdrachtgever SCAL. Persoonsgegevens mogen pas verwerkt worden indien:
**1.** Er geen twijfel bestaat dat betrokkene expliciet zijn toestemming heeft gegeven voor verwerking van zijn persoonsgegevens. Deze toestemming kan zowel schriftelijk als mondeling.[[10]](#footnote-10) Ten alle tijden kan betrokkende zijn toestemming weer intrekken. Dit heeft geen consequenties voor de gegevensverwerking vóór de intrekking van de toestemming[[11]](#footnote-11)Artikel 450 WGBO benoemt in lid 1 ook het toestemmingsvereiste van betrokkene. Dit is belangrijk voor de uitvoering van bijvoorbeeld een bloedonderzoek maar dus ook voor de bijbehorende registratie van persoonsgegevens.
Tevens geeft Artikel 458 WGBO een uitzondering op het toestemmingsvereiste genoemd in Artikel 8 sub a Wbp. De WGBO noemt de mogelijkheid om zonder toestemming van de cliënt ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van volksgezondheid de persoonsgegevens van cliënten (betrokkenen) te gebruiken. De verantwoordelijke kan inzage aan derden geven over het opgestelde dossier of inlichtingen over de cliënt delen. Wel worden er voorwaarden genoemd in lid 1 sub a en sub b: “*a. het vragen van toestemming in redelijkheid niet mogelijk is en met betrekking tot de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad, of
b. het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.*” De voorwaarden zijn streng en de mogelijkheden beperken zich alleen tot onderzoek waarbij toestemming vragen van cliënt het belang van het onderzoek zal schaden. Daarnaast mag het gegeven dat gedeeld wordt niet herleidbaar zijn naar de betreffende betrokkene. Tevens kan gebruik van gegevens zonder toestemming alleen als er ook nog aan de volgende criteria wordt voldaan genoemd in lid 2 van dit artikel: “*2. Verstrekking overeenkomstig lid 1 is slechts mogelijk indien:
a. het onderzoek een algemeen belang dient,
b. het onderzoek niet zonder de desbetreffende gegevens kan worden uitgevoerd, en
c. voor zover de betrokken patiënt tegen een verstrekking niet uitdrukkelijk bezwaar heeft gemaakt.”* Als betrokkene uit zichzelf nadrukkelijk heeft aangegeven geen gegevens ter beschikking te stellen tot wetenschappelijk onderzoek geldt dit artikel in ieder geval niet.
**2.** Een noodzaak bestaat voor het verwerken van persoonsgegevens zoals het uitvoeren van een overeenkomst waarbij betrokkene partij is. Of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van betrokkene en die noodzakelijk is voor het sluiten van een overeenkomst. Er mogen alleen relevante gegevens verwerkt worden voor het doel dat overeen is gekomen met betrokkene.
**3.** Er een noodzaak bestaat om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is.
**4**. De gegevensverwerking noodzakelijk is om een vitaal belang van betrokkene te garanderen.

***Rechten betrokkene(n)***
AP zal ten alle tijden op komen voor de rechten van betrokkenen. De volgende rechten worden expliciet genoemd in de wet- en regelgeving:
– Recht op informatie
Artikel 33 en 34 Wbp verplicht organisaties om betrokkene te informeren over wie zij zijn en dat zij zijn/haar persoonsgegevens zullen gebruiken. Het moet duidelijk zijn welke gegevens worden gebruikt en met wel beoogd doel. Indien diezelfde gegevens worden gedeeld met derden moeten zij betrokkene hiervan op de hoogte stellen.
De organisatie hoeft betrokkene niet in te lichten als er sprake is van onevenredige inspanning of als hij al op de hoogte is. Er kan sprake zijn van onevenredige inspanning als de organisatie informatie krijgt van een externe partner en heel veel moeite moet doen om bijvoorbeeld het woonadres van die persoon te achterhalen. Indien betrokkene al op de hoogte is via een externe partner dat de gegevens gedeeld gaan worden met een andere organisatie behoeft dit niet nogmaals geverifieerd te worden. Wel moet er geen twijfel bestaan over het feit dat betrokkene op de hoogte is.
Daarnaast beschrijft artikel 448 WGBO hetzelfde recht op informatie met betrekking tot een geneeskundige behandelovereenkomst. – Recht op inzage
Artikel 35 Wbp en Artikel 456 WGBO geeft betrokkene het recht om zijn persoonsgegevens in te zien. Dit geldt alleen voor zijn eigen gegevens en niet die van derden. Betrokkene kan ten alle tijden, zonder opgave van reden, de organisatie verzoeken zijn persoonsgegevens in te zien. De organisatie dient dan op duidelijke en begrijpelijke wijze in ieder geval het volgende te melden:
1. Of de organisatie zijn/haar gegevens gebruikt
2. Om welke gegevens het gaat
3. Met welk doel de gegevens worden gebruikt
4. Indien bekend wat de herkomst is van deze gegevens
5. Met wie de organisatie deze gegevens eventueel deelt
– Recht op correctie en verwijdering
Alhoewel Artikel 36 Wbp betrokkene het recht geeft om een correctie aan te brengen op zijn persoonsgegevens is hier door artikel 456 WGBO een nuance in aangebracht. Artikel 36 Wbp heeft het over het verbeteren, aanvullen, afschermen of verwijderen van gegevens. Echter wordt in de WGBO aangegeven dat men slechts een verbetering mag aan laten brengen als er sprake is van onjuiste notering van bijvoorbeeld een achternaam of geboortedatum. Voor al het overige mag betrokkene alleen verzoeken om een aanvulling als hij/zij het niet eens is met de hulpverlener. De correctie of aanvulling kan aangevraagd worden als de gegevens onjuist blijken te zijn, onvolledig zijn, niet ter zake doen voor het doel waarvoor het verzamelt is of op een andere manier in strijd is met wetgeving. Het correctierecht geldt niet voor kinderen onder de 16 jaar oud of mensen die onder curatele zijn gesteld. De wettelijke vertegenwoordiger kan dan in plaats voor henzelf verzoeken om een correctie.
– Recht van verzet
Artikel 41 Wbp geeft betrokkene het recht om de organisatie te verzoeken zijn/haar persoonsgegevens niet (meer) te gebruiken (recht van verzet). Dit recht is met name van toepassing op het gebruik van marketingdoeleinden. Maar kan ook gelden als betrokkene bijzondere persoonlijke redenen heeft om gebruik te maken van het recht van verzet. Het recht van verzet bij bijzondere persoonlijke omstandigheden staat omschreven in artikel 40 Wbp. Betrokkene dient het recht van verzet schriftelijk te verzoeken en toe te lichten aan de organisatie. Wat betreft het medische dossier dient men binnen drie maanden nadat het verzoek is ingediend door cliënt gehoor te geven aan de wens tot vernietiging van het dossier, aldus Artikel 455 WGBO.  ***Bewaartermijn***
De Wbp heeft geen concrete bewaartermijn van opgeslagen persoonsgegevens vastgelegd. Dit brengt met zich mee dat de verantwoordelijke zich dient af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Zijn er voldoende redenen dan kan hij bepalen welke termijnen gelden om die gegevens te bewaren. Voor de vastgestelde bewaartermijnen van persoonsgegevens dient men dus wel een goede motivatie hebben. Voor medische gegevens is de situatie anders. Artikel 7:454 lid 3 WGBO verplicht de hulpverlener (verantwoordelijke) een dossier aan te maken waarin de uitgevoerde handelingen en gegevens worden bewaard. Het dossier moet in ieder geval 15 jaren worden bewaard. Voor opdrachtgever SCAL geldt dit artikel omdat er sprake is van een geneeskundige behandelovereenkomst als er bloedonderzoek wordt verricht. Mocht betrokkene verzoeken de gegevens te verwijderen dan dient de verantwoordelijke hieraan gehoor te geven binnen een termijn van drie maanden[[12]](#footnote-12).  ***Onjuiste verwerking van persoonsgegevens***
De betrokkene kan zich zowel tot de verantwoordelijke als de bewerker wenden indien hij meent te zijn benadeeld bij de verwerking van zijn persoonsgegevens[[13]](#footnote-13). De verantwoordelijke is in eerste instantie aansprakelijk voor niet-naleving van de regels, door wie dan ook. De bewerker is slechts aansprakelijk voor eigen handelen. Dit zorgt er dan wel voor dat de verantwoordelijke ook de bewerker aansprakelijk kan houden voor zijn aandeel. Slechts wanneer verantwoordelijke of bewerker kunnen aantonen dat hun de schade niet kan worden aangerekend, gaan zij vrijuit. De bewijslast ligt in deze niet bij betrokkene. Tevens kan betrokkene via de rechter een verbod afdwingen om een bepaald persoonsgegeven te verwerken of te verwijderen. De verantwoordelijke dient hier gehoor aan te geven indien de rechter betrokkene in het gelijk stelt.

***Toezicht***In Nederland is de bevoegdheid tot het houden van toezicht op bescherming persoonsgegevens toebedeeld aan Autoriteit persoonsgegevens (Hierna te noemen AP)[[14]](#footnote-14). Naast een toezichthoudende functie heeft de AP ook een adviserende rol bij de ontwikkeling van beleidsregels en wet- en regelgeving omtrent bescherming persoonsgegevens.
Om onafhankelijkheid van de AP te waarborgen hoeft zij niet te voldoen aan alle artikelen van de Kaderwet zelfstandige bestuursorganen (hierna te noemen kaderwet)[[15]](#footnote-15). In de kaderwet is opgenomen dat de minister beleidsregels vaststelt met betrekking tot taakuitoefening van zelfstandig bestuursorganen (hierna te noemen Zbo). Tevens kan de minister een besluit van een Zbo vernietigen.[[16]](#footnote-16) Ondanks dat de AP een Zbo is heeft de minister geen bevoegdheden om invloed uit te oefenen op de beleidsregels die zij vaststelt.[[17]](#footnote-17).
De AP kan zelfstandig of op verzoek van een belanghebbende een onderzoek instellen bij een organisatie om de naleving van de wet en regelgeving te controleren[[18]](#footnote-18). Ten alle tijden zal AP inlichtingen verschaffen over haar bevindingen aan de belanghebbende(n) en verantwoordelijke(n). Mocht het nodig zijn wordt ook de betreffende minister op de hoogte gesteld.
Indien AP constateert dat de Wbp niet juist wordt nageleefd is zij bevoegd gebruik te maken van bestuursdwang[[19]](#footnote-19). De bestuurlijke boetes die momenteel opgelegd kunnen worden gaan tot een maximum van 4.500,- euro bij overtreding van Artikelen 27,28, 78 lid 2 onder a of 79 lid 1 van de Wet bescherming persoonsgegevens[[20]](#footnote-20). Zo geeft AP op hun eigen website de volgende toelichting[[21]](#footnote-21): “*Bestuurlijke boete als sanctie op niet nakomen van de meldingsverplichting
Deze bepaling kent aan de Registratiekamer in bepaalde gevallen de bevoegdheid toe om een bestuurlijke boete op te leggen. Het gaat om sanctionering van een beperkt aantal overtredingen die alle betrekking hebben op de verplichting om verwerkingen bij de Registratiekamer te melden. Concreet betreft het ten onrechte achterwege laten van de melding (artikel 27, eerste lid), het achterwege laten van de melding van een niet-geautomatiseerde verwerking voor zover onderworpen aan een voorafgaand onderzoek (artikel 27, tweede lid), het starten van de verwerking alvorens de melding heeft plaatsgevonden (artikel 27, derde lid), het doen van een onvolledige melding (artikel 28, eerste lid), het achterwege laten van de melding van het doel of de doeleinden waarvoor de gegevens of de categorieën van gegevens zijn verzameld, het niet of niet tijdig doorgeven van wijzigingen van de eerder gemelde gegevens (artikel 28, derde lid) en het niet vastleggen of bewaren van een specifieke categorie van verwerkingen (artikel 28, vierde lid). (II, nr. 3, blz. 188”*
De Wbp spreekt van een overtreding als men handelt in strijd met de wet en regelgeving en van een misdrijf als men deze overtreding met opzet overtreed. Indien er wordt geconstateerd dat men een misdrijf heeft begaan kan de verantwoordelijke een gevangenisstraf opgelegd krijgen van maximaal 6 maanden[[22]](#footnote-22).

De mogelijkheid tot het opleggen van sancties door de AP is van toepassing op het schenden van enkele artikelen uit de Wbp, *zie hiervoor bijlage1*. Deze artikelen hebben met name betrekking op de verplichting van een voorafgaand onderzoek (Hierna te noemen VO) alvorens men een persoonsnummer wil verwerken voor een ander doeleind (voor bijv. het koppelen aan een samenwerkende organisatie), het verwerken van strafrechtelijke gegevens en persoonsgegevens uit heimelijke observatie (bijv. camerabeelden). Mocht een organisatie bijvoorbeeld van plan zijn persoonsnummers te verwerken voor een ander doeleind dan beschreven in Artikel 8 lid 2 Wbp dan zijn zij verplicht een plan van aanpak op te stellen. Dit plan van aanpak dient door AP te worden getoetst. AP zal tijdens het VO toetsen of het plan wel aan de wettelijke vereisten voldoet.

3.1.2 Nieuwe Europese richtlijn
Mede omdat de maatschappij steeds meer digitale mogelijkheden heeft en daardoor de privacy van EU burgers steeds meer onder druk is komen te staan is besloten dat de oorspronkelijk Europese privacyrichtlijn niet meer voldoet. Daarnaast is het van belang om een uniform beleid te creëren op Europees niveau[[23]](#footnote-23). De Europese Commissie heeft op 25 januari 2012 voorstellen ingediend voor herziening van de richtlijn. Naar aanleiding van dit voorstel heeft de Europese Raad en het Europees Parlement veel vragen gesteld en aanpassingen (amendementen) doorgevoerd. Ook op Nationaal niveau zijn veel opmerkingen geplaatst door de tweede en eerste kamer (ook wel Nationaal Parement genoemd). Daarnaast heeft AP (toentertijd College bescherming persoonsgegevens) verschillende adviezen gegeven. Op 19 januari 2016 heeft de Europese Raad en het Europees Parlement het voorstel van de Europese Commissie, een verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, aangenomen. Dit betekent dat er een compromis is bereikt met alle lidstaten over de inhoud van de algemene verordening gegevensbescherming. Het zal nog enkele maanden duren voordat de privacy verordening officieel wordt aangenomen middels een stemming in de Europese Raad en het Europees Parlement. Pas na bekendmaking van de algemene verordening gegevensbescherming in het publicatieblad van de Europese Unie zal deze in werking treden. Er geldt een overgangstermijn van 2 jaren maar Nederland is al begonnen met voorbereidingen op implementatie van de verordening in de Nationale wet- en regelgeving. Zo geldt er bijvoorbeeld al een meldplicht op datalekken. In 2018 zal de Algemene verordening gegevensbescherming rechtstreekse werking hebben. In dit hoofdstuk kunt u hierover lezen en welke veranderingen nog meer doorgevoerd gaan worden in de Nationale wet- en regelgeving de komende twee jaar.
Het vervolg van dit hoofdstuk geeft de onderwerpen van de nieuwe algemene verordening gegevensbescherming aan.

***Datalekken***Voor de uitvoering van de meldplicht datalekken heeft AP beleidsregels opgesteld[[24]](#footnote-24). Deze beleidsregels zijn afgeleid van Artikel 31 verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[[25]](#footnote-25) (hierna te noemen algemene verordening gegevensbescherming). Belanghebbenden hadden tot 20 oktober 2015 de mogelijkheid om hier inspraak op te hebben. Na deze datum zijn de regels definitief geworden en gepubliceerd op de website van AP. Op 1 januari 2016 is in Nederland het meldplicht datalekken ingesteld.
De meldplicht datalekken is gericht op de verantwoordelijke. De verantwoordelijke is diegene die het doel van de middelen voor de verwerking van persoonsgegevens vaststelt[[26]](#footnote-26). Daarnaast duidt Artikel 13 Wbp de verantwoordelijkheid van de verantwoordelijke om passende veiligheidsmaatregelen te treffen bij verwerking van persoonsgegevens. Daarmee is het de grondslag van de meldplicht.
Artikel 33 tot en met Artikel 34a Wbp beschrijft wat een datalek is en welke actie verantwoordelijke moet nemen. Sprake van een datalek is er als onbedoeld persoonsgegevens vrijkomen, vernietigt of gewijzigd worden. Dus ook onrechtmatige verwerking van gegevens. De Wbp geeft geen termijn waarbinnen het datalek gemeld moet worden. Maar de beleidsregels van AP en Algemene verordening gegevensbescherming beschrijven een maximum van 72 uur waarbinnen de datalek na ontdekking gemeld moet zijn bij de toezichthouder[[27]](#footnote-27). Er mag geen sprake zijn van onnodige vertraging[[28]](#footnote-28). Artikel 34a lid 1 Wbp beschrijft dat er sprake is van een meldplicht als;
– de datalek aanzienlijke ernstige nadelige gevolgen voor bescherming persoonsgegevens oplevert
– of als er ernstige nadelige gevolgen ontstaan voor de bescherming van persoonsgegevens
– tevens geeft Artikel 34 a lid 2 Wbp de verplichting om de betrokkene waarvan persoonsgegevens zijn gelekt hier mede van op de hoogte te stellen. Echter is een belangrijke nuance aangebracht door de risico georiënteerde benadering[[29]](#footnote-29). De melding dient ook aan betrokkene worden gemeld als er waarschijnlijk ongunstige gevolgen zullen ontstaan voor de persoonlijke levenssfeer van die persoon. De toezichthouders van elk Europees land hebben samen een advies opgesteld waar voorbeelden worden genoemd.[[30]](#footnote-30)
Artikel 34a lid 8 Wbp beschrijft de plicht van de verantwoordelijke om een overzicht van elk datalek bij te houden in een register waarbij de volgende gegevens in ieder geval zijn genoteerd:
- feiten en gegevens rondom de aard van de inbreuk
- de tekst van kennisgeving aan betrokkene(n)
- instanties waar meer informatie te vinden is over de inbreuk
- aanbevolen maatregelen die de gevolgen van de betreffende inbreuk doen beperken
Naast de register datalekken, dient er ook een register te worden bijgehouden over de risico’s en evaluatie daarvan. Indien de evaluatie aangeeft dat er grote risico’s bestaan die de verwerkingsverantwoordelijke niet kan beperken met de beschikbare maatregelen, dient voor de verwerking om advies gevraagd te worden bij AP. Dit voor een zogenoemde gegevensbescherming effectbeoordeling[[31]](#footnote-31). De beoordeling dient ook verplicht aangevraagd te worden als er op grote schaal persoonsgegevens worden verwerkt. De verplichting voor deze beoordeling geldt niet, met betrekking op grootschalig verwerken, als het gaat om verwerking van persoonsgegevens van patiënten/cliënten door een individuele arts of zorgprofessional[[32]](#footnote-32).

***Functionaris voor gegevensbescherming***Met aanneming van de algemene verordening gegevensbescherming door de Europese Unie zal uiterlijk per het jaar 2018 voor enkele organisaties de verplichting gelden tot het instellen van een functionaris voor gegevensbescherming**.** Een ‘Data Protection Officer’ (hierna te noemen DPO) is een persoon die toezicht houdt op het verwerken van persoonsgegevens binnen een organisatie of afdeling. Deze functie bestaat al in Nederland maar wordt straks verplicht gesteld voor drie genoemde[[33]](#footnote-33) categorieën genoemd in Artikel 35 lid 1 verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens:
- publieke sector met uitzondering van gerechten
- indien sprake is van grootschalig monitoren van datasubjecten
- indien op grote schaal strafrechtelijke gegevens of andere bijzondere gegevens worden verzameld De organisatie die in bovengenoemde categorie valt dient aan de nationale autoriteit persoonsgegevens, in Nederland AP, kennisgeving te geven van benoeming van een DPO. De kans is aanzienlijk dat opdrachtgever SCAL een DPO dient in te stellen omdat zij op grote schaal bijzondere gegevens verwerkt. De inhoudelijke taken van een DPO worden in Artikel 37 lid 1 betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens beschreven:
- informeren en adviseren van de verantwoordelijke(n) over hun verplichtingen omtrent verwerking persoonsgegevens
- toezien op naleving van de algemene verordening gegevensbescherming[[34]](#footnote-34) en alle voortvloeiende beleidsregels met betrekking tot bescherming persoonsgegevens
- samenwerken met AP
- fungeren als aanspreekpunt/contactpersoon
Artikel 36 lid 3 beschrijft dat een DPO gedurende zijn werkperiode niet ontslagen of gestraft mag worden voor de uitvoering van zijn taken.
 ***Aanscherping toestemmingsvereiste***Toestemming van de betrokkene is al opgenomen in Artikel 8 lid 1 sub a Wbp en Artikel 450 WGBO. Toch lijkt het erop dat men middels de algemene verordening gegevensbescherming hier nog duidelijker in wil zijn. In de huidige Wet bescherming persoonsgegevens[[35]](#footnote-35) spreekt men al van ‘ondubbelzinnige toestemming’. In de Algemene verordening gegevensbescherming spreekt men over een vrijelijk gegeven toestemming. Dit houdt in dat de toestemming geen geldige grondslag mag zijn voor de verwerking van persoonsgegevens als er sprake is van een duidelijke onevenwichtigheid tussen betrokkene en verwerkingsverantwoordelijke[[36]](#footnote-36). Dit kan zich voordoen bij bijvoorbeeld overheidsinstanties. Daarnaast moet er voor elk verwerkingsdoel apart toestemming worden gegeven. Tevens beschrijft de Algemene verordening gegevensbescherming dat toestemming moet worden gegeven door een ondubbelzinnige actieve handeling, zoals een schriftelijke of mondelinge verklaring. Maar een vakje aankruisen op een website voldoet ook. Wel moet er ten alle tijden aan goede informatievoorziening worden voldaan. De verwerkingsverantwoordelijke moet kunnen aantonen dat betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Hieruit moet blijken dat betrokkene bewust was van het geven van toestemming en hoever deze toestemming reikt.[[37]](#footnote-37)

***Aanscherping informatievoorziening***

In de huidige wetgeving genoemd in Artikel 33 Wbp wordt al gesproken van de verplichting van informatievoorziening door verwerker aan betrokkene. Waar in dit artikel wordt gesproken over “nadere informatie” spreekt de nieuwe privacy verordening over het verschaffen van “beknopte, transparante, begrijpelijke en makkelijk toegankelijke vorm en in duidelijke en

eenvoudige taal informatie”[[38]](#footnote-38). Daarnaast wordt in het bijzonder rekenschap in communicatie van informatie naar kinderen toe genoemd. De informatie dient schriftelijk indien gebruikelijk elektronisch verschaft aan betrokkene. Op verzoek van betrokkene kan de informatie mondeling worden verstrekt nadat de identiteit van betrokkene is vastgesteld.
Tevens benoemt Artikel 13 lid 1 Verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens inhoudelijke toevoegingen aan de verplichte informatievoorziening[[39]](#footnote-39):
- naast de identiteit en contactgegevens van verwerker dient nu ook de identiteit en contactgegevens van de functionaris privacybescherming gemeld worden (indien van toepassing)
- naast benoeming van de doelen waarvoor de gegevens van betrokkene worden gebruikt is de verwerker nu ook verplicht om betrokkene te wijzen op de rechtsgrond van dat doel
- en de gerechtvaardigde belangen van de verwerker dienen te worden gemeld
Ook heeft de verantwoordelijke de plicht om betrokkene op zijn rechten te wijzen met betrekking tot verwerking van zijn persoonsgegevens.
- de risico’s met betrekking tot het verwerken van de persoonsgegevens dienen kenbaar te worden gemaakt.
Om nog meer ondersteuning te bieden met betrekking tot het geven van informatie, zijn er privacy-iconen ontwikkelt, *zie hiervoor bijlage* *2*. Deze iconen moeten niet maar mogen gebruikt worden door de lidstaten.

***Recht om vergeten te worden***In de algemene verordening gegevensbescherming wordt veel aandacht geschonken aan de rechten van betrokkene(n). Het recht om vergeten te worden bestaat momenteel al vanwege het zogenaamde Google-arrest. Om er voor te zorgen dat de lidstaten hun privacy richtlijnen conform de Europese richtlijnen opstellen bestaat de mogelijkheid tot het aanvragen van een prejudiciële beslissing van het Europees Hof door nationale rechters. Het Europees Hof zal toetsen of de implementatie van het Europees recht naar het nationale recht van de lidstaat wel voldoet. In 2014 heeft het Hof van Justitie een prejudiciële beslissing genomen over de uitleg van artikelen 2, sub b en d, 4, lid 1, sub a en c, 12, sub b, en 14, eerste alinea, sub a van richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en van artikel 8 van het Handvest van de grondrechten van de Europese Unie. Eén van de prejudiciële vragen betrof ‘het recht om vergeten te worden’(hierna te noemen ‘Google- arrest).[[40]](#footnote-40) De heer Costeja had zoekmachine Google verzocht om bepaalde zoekresultaten van hem te verwijderen. Op basis van de huidige privacyrichtlijn, o.a. opgenomen in de Wet bescherming Persoonsgegevens, kan Google inderdaad verplicht worden bepaalde gegevens te verwijderen. Als de persoonsgegevens onnauwkeurig, ontoereikend, niet ter zake dienend of bovenmatig zijn voor de doeleinden van de verwerking, omdat niet bijgewerkt of omdat langer bewaard dan noodzakelijk is, tenzij de bewaring ervan is vereist wegens historische, statistische of wetenschappelijke doeleinden.[[41]](#footnote-41)

In de Algemene verordening gegevensbescherming wordt het recht om vergeten te worden nog scherper opgenomen[[42]](#footnote-42). De verwerkingsverantwoordelijke dient betrokkene te wijzen op de mogelijkheden die men heeft om dit recht uit te voeren. Zowel het recht om vergeten te worden als verzoeken om inzage, wijzigingen of bezwaar indienen. Er moeten procedures voor handen zijn om dit recht door betrokkene juist uit te kunnen laten voeren. Daarnaast dienen deze middelen ook elektronisch voor handen te zijn, zeker als de persoonsgegevens via een elektronische weg worden verwerkt. De verwerkingsverantwoordelijke is verplicht om zo spoedig mogelijk gehoor te geven aan het verzoek van betrokkene. In ieder geval binnen een termijn van één maand[[43]](#footnote-43).

***Vastleggen administratieve handelingen***Naast versterking van de rechten van betrokkene(n) zijn er ook meer administratieve handelingen beschreven in de algemene verordening gegevensbescherming. Eerder is genoemd het bijhouden van registers omtrent risico’s en datalekken.
Zo ook dient te worden vastgelegd welke afspraken zijn gemaakt met de verwerkingsverantwoordelijke[[44]](#footnote-44). Elke handeling die de verwerkingsverantwoordelijke uitvoert dat betrekking heeft op verwerking van persoonsgegevens dient te worden beschreven. Daarbij dient expliciet de bijkomende verantwoordelijkheid en aansprakelijkheid te worden vastgelegd. Er moet een verplichting gelden voor de verwerkingsverantwoordelijke om passende maatregelen te nemen om de uitoefening van de algemene verordening gegevensbescherming correct uit te oefenen. Dit moet hij/zij tevens kunnen aantonen doormiddel van het bijhouden van een register. In dit register moet elke uitgevoerde handeling met betrekking tot verwerking van persoonsgegevens worden bijgehouden. Dit register dient ten alle tijden verstrekt te worden indien AP hierom verzoekt[[45]](#footnote-45). Bij het uitvoeren van deze beschreven maatregelen dient rekenschap te worden gehouden met de aard, context, risico voor de rechten en vrijheden van natuurlijke personen, het doel en de omvang. In de algemene verordening gegevensbescherming wordt de belangrijkheid voor het beschermen van onder andere medische gegevens nog eens extra onderstreept[[46]](#footnote-46). Tevens wordt aangemoedigd dat men zich als verwerkingsverantwoordelijke, om aan te tonen dat er aan de verplichtingen worden voldaan, aan zou kunnen sluiten bij een gedragscode of goedgekeurde certificeringsregeling[[47]](#footnote-47). Dit zou een belangrijk middel kunnen zijn om aan te tonen dat er aan de voorwaarden zijn voldaan.
Bovenstaande moet schriftelijk worden vastgelegd door middel van een overeenkomst of opname in de bepalingen van het contract. De modelovereenkomst dient te worden ontwikkelt en aangereikt door de Commissie of AP.

***Uitbreiding bevoegdheden van de AP***
In Nederland bestaat een onafhankelijke toezichthoudende autoriteit namelijk AP. Het belang van zo’n toezichthouder wordt meerdere keren genoemd in de algemene verordening gegevensbescherming en wordt nu ook verplicht gesteld.[[48]](#footnote-48) Dit heeft tot gevolg dat de bevoegdheden van AP uitgebreid en aangescherpt worden. De Algemene verordening gegevensbescherming beschrijft de specifieke taken van de toezichthoudende autoriteit[[49]](#footnote-49):
- Behandelen van klachten ingediend door betrokkene(n)
- Een breder publiek bekend maken met de risico’s, voorschriften, rechten omtrent de verwerking van persoonsgegevens
- Evalueren van de toepassing van de verordening
- Toezicht houden op de toepassing van de verordening

De bevoegdheden dienen onpartijdig, eerlijk en binnen een redelijk termijn te worden uitgevoerd.
Tevens wordt aangegeven dat de toezichthoudende autoriteit de bevoegdheid heeft bindende besluiten te nemen als het gaat over maatregelen ter toepassing van de verordening. De maatregelen dienen passend, overeenkomstig met de algemene verordening gegevensbescherming, rekening houdend met elk individueel geval, noodzakelijk en overbodige kosten en buitensporige ongemakken voor betrokkenen personen te vermijden. Ook dient het recht van iedere persoon eerbiedigt te worden door alvorens het besluiten tot het nemen van een maatregel, die voor hem nadelige gevolgen zal hebben, te horen.
Er kunnen zich situaties voordoen waarbij de toezichthoudende autoriteit direct moet ingrijpen alvorens een definitieve beslissing wordt genomen. Om de rechten en vrijheden van betrokkene(n) te beschermen omdat deze aanzienlijk worden aangetast, kan AP voorlopige maatregelen treffen voor een maximale duur van 3 maanden.

***Sancties AP***
AP heeft in Nederland al de bevoegdheid om bestuurlijke boetes op te leggen indien sprake is van dergelijke overtredingen. De algemene verordening gegevensbescherming wil met het oog op een strengere handhaving van regels dat er bij elke overtreding straffen en/of boetes worden opgelegd. Deze boetes en straffen moeten gezamenlijk met de maatregelen worden opgelegd. Wel is er een nuance aangebracht indien er sprake is van een kleine inbreuk of een onevenredige last voor een natuurlijk persoon. Dan mag er in plaats van een geldboete worden gekozen voor een berisping[[50]](#footnote-50). Hoe hoog de geldboetes en straffen zijn kan verschillen per lidstaat. Nederland kan deze normen zelf vaststellen aan de hand van nationale wetgeving[[51]](#footnote-51). Maar er is wel een maximum vastgesteld voor de hoogte van deze boetes in de algemene verordening gegevensbescherming[[52]](#footnote-52). Zo beschrijft Artikel 79 lid 3 van de algemene verordening gegevensbescherming dat geldboetes tot maximaal 10.000 euro of voor een onderneming tot 2 % van de jaaromzet in het voorgaande boekjaar mits deze hoger is dan 10.000 euro. Tevens beschrijft Artikel 79 lid 3 Algemene verordening gegevensbescherming in welke situaties sprake is van schending van de verscheidende artikelen.

***Mogelijkheid tot een samenwerkingsprotocol***
Tevens heeft AP de mogelijkheid gekregen om samen te werken met andere toezichthouders aan de hand van een samenwerkingsprotocol. Dit om het belang van efficiënt en effectief toezicht houden op de verwerking van persoonsgegevens te kunnen waarborgen[[53]](#footnote-53). Dit samenwerkingsprotocol wordt altijd gepubliceerd in het Staatscourant[[54]](#footnote-54). Momenteel is alleen AP een toezichthoudende autoriteit voor bescherming persoonsgegevens maar dit zal in de toekomst kunnen veranderen.

3.1.3 Toepassing huidige wet- en regelgeving en de nieuwe algemene verordening gegevensbescherming op SCAL
Opdrachtgever SCAL is een organisatie die zich toegelegd heeft op het uitvoeren van diagnostisch onderzoek. Tijdens het verwerken van de persoonsgegevens die bij een bloedonderzoek worden gebruikt heeft SCAL een aantal doelen[[55]](#footnote-55) in aanmerking te nemen:
– Controleren of het geplande onderzoek bij de juiste persoon wordt uitgevoerd (mede om fraude te voorkomen)
– Voldoen aan de zorgplicht vanuit de WGBO[[56]](#footnote-56) en de Wbp[[57]](#footnote-57)
– Onderzoek op een correcte wijze uitvoeren
– Zorgen voor een juiste doorverwijzing indien nodig
– Een externe opdracht uitvoeren ten behoeve van de cliënt (doorverwijzing naar SCAL voor diagnostisch onderzoek)

Bij elk diagnostisch onderzoek dat bij SCAL plaatsvindt wordt een overeenkomst gesloten tussen verantwoordelijke en betrokkene middels een aanmeldformulier. De verantwoordelijke draagt zorg dat de betrokkene op de hoogte is van de aangegane overeenkomst en ook uitlegt voor welke doeleinden bepaalde handelingen worden uitgevoerd. Er mogen alleen relevante gegevens worden verwerkt voor het doel dat overeen is gekomen met de betrokkene. Een aantal medewerkers, artsen en verpleegkundigen[[58]](#footnote-58), van SCAL staan tevens geregistreerd in het BIG register. Dit brengt een aantal rechten en plichten met zich mee die genoemd staan in de Wbp, WGBO en BIG.
Eén van de diagnostische onderzoeken is bloedonderzoek. Om bloed te onderzoeken moet dit eerst worden verkregen via veneuze bloedafname bij betrokkene. Alleen de verpleegkundige en/of arts, die BIG-geregistreerd staat, mag deze voorbehouden handeling uitvoeren. Het bloed dat wordt afgenomen wordt gekenmerkt als een bijzonder persoonsgegeven. Dit omdat er sprake is van een medisch persoonsgegeven. De rest van de informatie die opgevraagd en verwerkt wordt over betrokkene zijn persoonsgegevens. Zo wordt onder andere gecontroleerd wie de persoon is en of deze persoon verzekerd is. Omdat opdrachtgever SCAL vaak in opdracht van externe partijen werkzaam is en haar declaratie direct naar de verzekeraar wilt toesturen dient zij aan wettelijke verplichtingen te voldoen. Zo stelt Artikel 87 van de zorgverzekeringswet dat de zorgaanbieder verplicht is de noodzakelijke persoonsgegevens, waaronder die betreffende de gezondheid van de verzekerde (betrokkene), te verstrekken. Noodzakelijk betekent in deze alleen de gegevens die nodig zijn om de declaratie rond te kunnen krijgen. Men dient bijvoorbeeld te weten of de betrokkene verzekerd is voor een bepaald onderzoek of dat dit buiten zijn polis valt. En een BSN-nummer is noodzakelijk om de betrokkene te kunnen identificeren.

Het is van belang dat opdrachtgever SCAL rekening houdt met de invoering van de nieuwe Europese wet- en regelgeving. De Algemene verordening gegevensbescherming heeft rechtstreekse werking en zal na de overgangstermijn in 2018 in werking treden. Voor de medewerkers die handelingen verrichten waarbij persoonsgegevens worden verwerkt is het belangrijk dat zij wetenschap hebben van de (komende) veranderingen en aanscherpingen. Gedurende het uitvoeren van bloedonderzoek dienen zij zich bewust te zijn van:

***Informatieplicht***
De informatie die zij met de cliënt delen over de uit te voeren handelingen, aldus Artikel 12 Algemene verordening gegevensbescherming. De informatie dient schriftelijk of digitaal te worden verstrekt en op verzoek mondeling nog eens toegelicht. Artikel 14 Algemene verordening gegevensbescherming beschrijft concreet welke informatie in ieder geval dient te worden medegedeeld aan betrokkene. Identiteit en contactgegevens van de verwerkingsverantwoordelijke, beoogde doel van de verwerking persoonsgegevens, hoelang de persoonsgegevens bewaard blijven, inlichting over het recht van verzet, correctie en inzage van betrokkene, inlichting over het recht om een klacht in te dienen door betrokkene, contactgegevens van de privacy functionaris als men die heeft binnen de organisatie. Al deze informatie dient ook op een digitale wijze beschikbaar te zijn. Tevens dient opdrachtgever SCAL betrokkene inlichtingen te verschaffen als men van plan is persoonsgegevens voor andere doeleinden te gebruiken dan is overeengekomen. Dit gaat met name om het gebruik van afgenomen monsters voor wetenschappelijk onderzoek. Voorheen was het voldoende om te vragen of cliënt bezwaar heeft tegen gebruik van lichaamsmateriaal voor wetenschappelijk onderzoek. Tegenwoordig dient gemeld te worden of er wetenschappelijk onderzoek gedaan wordt binnen de organisatie en op welke wijze.

***Toestemmingsvereiste***
Wanneer men mag spreken van toestemming, aldus Artikel 7 Algemene verordening gegevensbescherming. Tevens is Artikel 9 Algemene verordening gegevensbescherming in het bijzonder van toepassing omdat men hier voorwaarden stelt voor de toestemmingsvereiste van bijzondere persoonsgegevens. Uitgangspunt is dat het verboden is om medische persoonsgegevens te verwerken mits betrokkene uitdrukkelijk zijn toestemming gegeven heeft voor het beoogde doel waarvoor de medische gegevens worden verwerkt. SCAL dient ten alle tijden te kunnen aantonen dat cliënt akkoord is gegaan met het verwerken van de persoonsgegevens voor het beoogde doel dat alvorens is besproken met cliënt.

***Administratieve handelingen***
Een goed privacy beleid op papier en in de uitvoering is noodzakelijk maar dit dient ook aangetoond te kunnen worden:
- Er dient een register van verwerkingsactiviteiten te bestaan, aldus Artikel 28 Algemene verordening gegevensbescherming. Hier dient onder andere in opgenomen te staan wat de contactgegevens zijn van de verwerkingsverantwoordelijke, beoogde doel(en) voor de verwerking persoonsgegevens, welke betrokkene en welke categorie persoonsgegevens het betreft, met wie de persoonsgegevens gedeeld zullen worden, hoe lang de persoonsgegevens bewaard worden, indien mogelijk een beschrijving van de genomen technische en organisatorische beveiligingsmaatregelen.
- De resultaten van uitgevoerde risico analyses dienen vastgelegd te worden. Hierin dient onder andere in beschreven te worden welke risico’s zijn gesignaleerd en welke acties ondernomen zijn om de risico’s te beperken.
- Datalekken, klein of groot, dienen te worden vastgelegd.
- De directie van SCAL moet kunnen aantonen welke afspraken gemaakt zijn met de verwerkingsverantwoordelijke en bewerker. Welke taken en bevoegdheden gelden voor de leidinggevenden en welke voor het personeel dat onder zijn/haar toezicht handelingen verricht. Dit kan middels opname in een arbeidscontract of aparte functiebeschrijving, verplichte certificering of gedragscode.

***Instellen privacyfunctionaris***
Artikel 24 Algemene verordening gegevensbescherming geeft aan dat het de verantwoordelijkheid van de directeur en directe leidinggevende is dat de medewerkers die betrokken zijn bij het diagnostische onderzoek goed geïnstrueerd zijn. Tevens dient de directeur uit te zoeken of de verplichting van het aanstellen van een privacy functionaris noodzakelijk is. Deze functionaris kan ingezet worden voor het opstellen en handhaving van het privacy beleid. Gedurende het uitvoeren van bloedonderzoek worden met name bijzondere persoonsgegevens, namelijk medische gegevens, verwerkt. Artikel 35 lid 1 sub c Algemene verordening gegevensbescherming geeft aan dat het aanwijzen van een privacy functionaris in ieder geval aangewezen dient te worden als men op grote schaal bijzondere persoonsgegevens verwerkt. Omdat SCAL ook een organisatie is dat op grote schaal bijzondere persoonsgegevens, namelijk medische gegevens, verwerkt is de kans groot dat zij een privacy functionaris dienen aan te stellen.

3.2 Documentenanalyse
Op basis van document analyse bij SCAL is onderzocht of de beleidsregels van SCAL op dit moment al voldoen aan de aanscherping van de richtlijnen in de Algemene verordening gegevensbescherming.
Opdrachtgever SCAL heeft een geschreven beleid middels het computerprogramma ‘Wiki’. Alleen medewerkers hebben toegang tot ‘Wikki’ en kunnen de opgenomen documenten lezen. Zo is het beleid binnen de organisatie opgenomen in het kwaliteitshandboek Salux healthcare[[59]](#footnote-59) en het privacy reglement Salux healthcare Leiden terug te lezen op Wiki.[[60]](#footnote-60) Daarnaast zijn er de SOP(Standard Operating Procedure)documenten. Die geven meer informatie over bepaalde uitvoeringshandelingen en de wijze waarop deze dienen te worden uitgevoerd. De SOPdocumenten zijn opgesteld door de leidinggevende van een bepaalde afdeling (zoals de klinisch chemicus van het laboratorium), medewerkers van kwaliteit of de directeur zelf. Het geschreven beleid die opdrachtgever SCAL gebruikt wordt beschreven. Getoetst wordt of dit beleid (nog) voldoet aan de wet- en regelgeving betreffende bescherming persoonsgegevens.
 ***Kwaliteitshandboek Salux Healthcare***Het kwaliteitshandboek Salux healthcare[[61]](#footnote-61) is specifiek gericht op het laboratorium en wordt gebruikt als richtlijn voor de uitgevoerde werkzaamheden waaronder bloedonderzoek. Het handboek is geldig tot 01 januari 2019. Bij bestudering van het handboek valt op dat er weinig relevant is voor het privacy beleid. Voornamelijk wordt er in gegaan op de inhoud en kwaliteit van een diagnostisch onderzoek. Toch zijn er enkele hoofdstukken op (in)directe wijze van belang voor het onderzoek naar het privacy beleid binnen SCAL.

*Hoofdstuk 2 Normatieve verwijzing* geeftaan op welke wet- en regelgeving het handboek gebaseerd is. De wet BIG, Kwaliteitswet zorginstellingen (is komen te vervallen per 01 januari 2016), WGBO, Wet Klachtrecht Cliënten Zorgsector (is komen te vervallen per 01 januari 2016), Wet bescherming persoonsgegevens zijn relevant voor het onderzoek. Zoals te lezen is dat twee van deze wetgevingen zijn komen te vervallen en de overige wetgeving aangepast zal worden met de komst van de Algemene verordening gegevensbescherming.

*Hoofdstuk 4.1 Verantwoordelijkheid van de organisatie en het management* beschrijft dat de directie de eindverantwoordelijkheid draagt voor de uitvoering van de door hen opgestelde richtlijnen. Dit is in overeenstemming met Artikel 25 Algemene verordening gegevensbescherming.
De werkprocessen worden vastgelegd in de eerder genoemde SOP-documenten. Hier verwijst het handboek dan ook naar. Dit alles is niet specifiek op bescherming van persoonsgegevens gericht. Tevens lijken de SOPdocumenten en alle overige documenten op HBO-niveau geschreven. De vraag die gesteld kan worden is of om deze reden de documenten wel toegankelijk genoeg zijn voor alle medewerkers. In dit kwaliteitssysteem zijn de volgende documenten relevant voor het onderzoek naar het privacy beleid binnen SCAL: SOP documenten, verkorte werkvoorschriften, rapporten ,controlekaarten en checklisten.

*Hoofdstukken 4.2 t/m 4.*12 Kwaliteitsmanagementsysteem is relevant voor het vaststellen van dienstverleningsovereenkomsten. Een dienstverlenersovereenkomst kan worden opgevat als de behandelovereenkomst die de cliënt op dat moment aan gaat met diegene die het bloed afneemt en diegene die vervolgens het bloed onderzoekt.
De dienstverleningsovereenkomst is het papieren aanvraagformulier of digitaal via zorgdomein. Een dienstverlenersovereenkomst wordt gebruikt voor het doen van bloedonderzoek omdat dit als een medische handeling wordt gezien.
Op het aanvraagformulier staan verschillende invulvelden die verplicht dienen te worden ingevuld. Zo dient de naam, adres/contactgegevens, BSN-nummer, geboortedatum en geslacht te worden opgeschreven. Ook is er een mogelijkheid voor de cliënt om aan te geven dat hij bezwaar heeft tegen ander gebruik van zijn lichaamsmateriaal als waarvoor het is afgenomen. De aanvrager is verantwoordelijk voor de correctheid van de ingevulde gegevens. Door het aanvraagformulier in te leveren gaat de cliënt akkoord met de algemene voorwaarden. Wat deze voorwaarden zijn is niet duidelijk en ook niet aangegeven op het aanvraagformulier. Zowel het aanvraagformulier als het afgenomen materiaal worden gekenmerkt met een uniek labnummer met tijdstip en datum van ontvangst. Voor overige instructies over het aannemen van een aanvraag wordt verwezen naar een SOPdocument.[[62]](#footnote-62) Uitslagen zijn opgenomen in rapporten waarin de volgende relevante onderdelen zijn opgenomen: identificatie cliënt (geboortenaam, minimaal één letter van de voornaam, geboortedatum en adres) op elke bladzijde, identificatie van de aanvrager, identificatie laboratorium, onderzochte waardes, uitslagen, monstertype, afnamedatum en identificatie van de persoon(en) die de resultaten hebben beoordeelt. Op de website van opdrachtgever SCAL[[63]](#footnote-63) is informatie te vinden met betrekking tot het doen van een aanvraag voor diagnostisch onderzoek. Het handboek verwijst naar de website maar niet vanwege het privacy beleid. Wel wordt er onder het kopje privacy, op de website, het volgende gemeld: *“De medewerkers van SCAL Medische Diagnostiek hebben geheimhoudingsplicht ten aanzien van de patiënt- en onderzoeksgegevens. Tot de regels van het privacyreglement in het kader van de Wet Bescherming Persoonsgegevens behoren alle gegevens gerelateerd aan patiënten en onderzoeksresultaten. Alle medewerkers van SCAL hebben een verklaring ondertekend dat men kennis heeft genomen van de regels met betrekking tot de geheimhoudingsplicht van patiëntgegevens.”*De website van SCAL fungeert als informatiebron voor zowel cliënten als aanvragers. Er wordt gesproken over een ABC lijst waarin onder andere de bewaartermijnen te lezen zijn. Deze lijst is bij nader onderzoek niet op de website terug te vinden. Men kan folders over bijvoorbeeld bloedonderzoek downloaden. Wel moet er eerst verplicht een aantal contactgegevens worden ingevuld (naam, achternaam en postcode). Daarnaast moet er een aanvragerscode worden ingevuld. Hoe men aan deze code kan komen is onduidelijk. Wel staat aangegeven dat de privacy van persoonlijke informatie van cliënten op de website is beschreven.
Uitslagen van gedane onderzoeken worden na autorisatie automatisch in het laboratoriuminformatiesysteem genoteerd. Het overgrote deel van de uitslagen worden gedeeld via Sleutelnet naar het Huisarts Informatie Systeem. Voor een kleiner deel worden de uitslagen per post gedeeld met de aanvragers en eventueel op verzoek van de aanvrager gefaxt. Wel wordt dan contact opgenomen met de aanvrager om te controleren of de fax daadwerkelijk ontvangen is.
Het is mogelijk voor de cliënt om een kopie van de uitslagen te ontvangen tegen betaling van de gemaakte administratieve kosten. Tevens dient de cliënt zich te kunnen identificeren als zijnde de persoon bij wie het onderzoek is verricht. Wijzigingen of aanvullingen van gerapporteerde uitslagen worden indien noodzakelijk telefonisch gemeld waarna een herziende rapportage wordt afgedrukt en verzonden naar de aanvrager. Op welke wijze wordt niet genoemd.
Voor de instructies betreft het rapporteren en delen van uitslagen wordt verwezen naar een aantal SOPdocumenten.

*Hoofdstukken 4.13 t/m 4.15 Registraties en preventie* worden het beheer van registraties, corrigerende en preventieve maatregelen en risicomanagement toegelicht. Bij de uitvoering van activiteiten worden registraties gelijktijdig opgesteld door de medewerkers. Deze registraties kunnen logboeken, parafering op documenten, digitale vastlegging van onderzoeksresultaten, rapporten enzovoorts zijn. De registraties zijn beschermd tegen onbevoegde wijzigingen. In één van de SOPdocumenten[[64]](#footnote-64) staan de bewaartermijnen van deze registraties (documenten) genoteerd. Met betrekking tot het privacy beleid is het relevant weet te hebben van wat er wordt geregistreerd: aanvraag voor onderzoek, registratie van het aannemen van een aanvraag, onderzoeksresultaten en rapporten. Tevens worden registraties bijgehouden van controles, incidenten, incidentenoverzichten, risicomanagement, klachten en corrigerende en preventieve maatregelen die genomen worden.
De kwalificaties, opleiding en competentieregistratie en bevoegdheden van medewerkers worden vastgelegd in het personeelsdossier. Tijdens het jaargesprek worden deze zaken doorgesproken met de medewerker. Deze informatie is van belang voor de medewerker zodat hij/zij weet wat er van hem/haar mede verwacht wordt rondom privacy beleid.
In het personeelsdossier wordt er naast het functieprofiel en andere zaken ook een bekwaamheidsverklaring en geheimhoudingsverklaring bewaard.
Over de laboratorium en kantoorfaciliteiten wordt het volgende gezegd. De prik- en onderzoeksruimtes zijn af te sluiten om de privacy van cliënten te kunnen waarborgen. Tevens wordt aangegeven dat er een mogelijkheid dient te bestaan voor het blinderen van de ramen en deuren van de prikruimte. Ondertussen wachten de andere cliënten in een wachtruimte. Bezoekers hebben geen toegang tot andere ruimtes zonder begeleiding. De toegang tot de niet-publieke ruimtes is afgesloten en beveiligd met een elektronisch systeem. Toegang tot computers is alleen toegestaan als hiervoor opdracht is gegeven door HR of een afdelingshoofd. Hierdoor wordt onbevoegd toegang tot patiëntengegevens voorkomen. De computers zijn voorzien van een wachtwoordbeveiligingssysteem. Bij het verlaten van de werkplek dient uitgelogd te worden door de betreffende werknemer.
In de kelder bevindt zich onder andere het archief waar documentatie wordt bewaard. Voor de wijze van archiveren, bewaartermijnen en vernietigen van documenten wordt verwezen naar een SOPdocument.[[65]](#footnote-65) Tevens staat er een koelkast dat voorzien is van een logger.

***SOPdocumenten***
Elk document heeft een code en titel gekregen waardoor ze goed terug te vinden zijn. Tevens zijn ze op alfabetische volgorde opgenomen in de lijst met sopdocumenten. De documenten zijn uniform opgesteld met dezelfde ondertitels hierdoor kan men in één oogopslag vinden wat relevant is. Zo wordt het doel van het document beschreven, eventuele voorzorgsmaatregelen, verantwoordelijkheden en procedure waarin de handelingen uitgeschreven zijn. De teksten zijn geschreven op HBO niveau. In totaal bestaan er 15 documenten, zie bijlagen, die van toepassing zijn op het bloedonderzoek. Met deze documenten worden een aantal handelingen nader beschreven.
*Aannemen van een aanvraag*[[66]](#footnote-66)[[67]](#footnote-67)In de volgende SOPdocumenten kunnen medewerkers lezen hoe te handelen bij het aannemen van een aanvraag: baliewerkzaamheden en aannemen van een aanvraag, *zie hiervoor bijlagen 3A en 3B*. Uitgelegd wordt hoe een aanvraagformulier moet worden gecontroleerd en indien nodig gegevens moeten worden aangevuld of gecorrigeerd. Tevens staat genoteerd dat de medewerker rekening dient te houden met de privacy van cliënt. Op welke wijze hier rekenschap mee moet worden gehouden wordt niet genoemd. Bij beschrijving van de procedure wordt beschreven dat de cliënt zich bij de balie dient te melden met het aanvraagformulier en legitimatiebewijs. De medewerker dient de cliënt met de foto op het afgegeven legitimatiebewijs te controleren. Tevens wordt gecontroleerd of het BSN nummer overeen komt met de opgeschreven BSN nummer op het aanvraagformulier. Na controle van de geboortedatum worden de NAW gegevens gecheckt.
De ziektekostenverzekering moet ook worden gecontroleerd, dit gaat middels het verzekeringspasje die cliënt bij zich moet hebben. Als de cliënt dit niet bij zich heeft dan worden zijn verzekeringsgegevens opgezocht in een computersysteem. Bij de beschrijving wordt niet genoemd dat hiervoor toestemming moet worden opgevraagd bij de cliënt. In het SOPdocument, *zie hiervoor bijlage* 3C “gegevens van verzekerden opvragen en controleren[[68]](#footnote-68)” wordt beschreven dat de volgende gegevens van verzekerde cliënten kan worden opgevraagd: voorletter en achternaam, adres en woonplaats, geboortedatum, zorgverzekeraar, verzekeringsnummer, BSN nummer en unieke zorgverzekeraars identificatie (Uzovi-nummer).
In de SOPdocumenten waarin beschreven wordt hoe te handelen bij een aanvraag voor onder andere bloedonderzoek wordt niet beschreven welke informatie met cliënt gedeeld dient te worden en op welke wijze toestemming gevraagd moet worden voor de handelingen die verricht gaan worden. Eerder was te lezen in het kwaliteitshandboek Salux Healthcare dat de cliënt toestemming geeft door het inleveren van het aanvraagformulier. En dat dit ook gekenmerkt wordt als de dienstverleningsovereenkomst die de cliënt met SCAL aan gaat.
*Doorgeven uitslagen*[[69]](#footnote-69)
In het SOPdocument rapportage, *zie bijlage 3D*, wordt uitgelegd op welke wijze resultaten van onder andere een bloedonderzoek moeten worden doorgegeven aan de aanvrager. Hierin staat beschreven dat men uitslagen op diverse wijze kan delen met de aanvrager: Elektronische rapportage via fax of sleutelnet, per post of mondeling per telefoon. Als men een uitslag per fax verzend dan wordt aan het einde van de dag middels een print van alle verstuurde faxrapporten bekeken of de verzending goed is verlopen. De werknemer dient op de print een paraaf te noteren en eventuele bijzonderheden te noteren. Deze print wordt bewaard in een ‘klapper gefaxte resultaten’. Uit het SOPdocument is op te merken dat de uitslagen alleen doorgebeld worden als er een sterke afwijking geconstateerd is in de resultaten van het bloedonderzoek. Wel worden deze uitslagen ook nog eens gefaxt naar de betreffende aanvrager. Middels een doorbellijst wordt bijgehouden met wie er gesproken is en op welk tijdstip. Mocht er sprake zijn van een telefonisch verzoek van de aanvrager om een uitslag dan dient de werknemer alvorens om een artsencode te vragen. Indien de artsencode niet overeenkomt met die op het aanvraagformulier dient de werknemer met de klinisch chemicus te overleggen of de uitslag alsnog doorgegeven mag worden.
*Archiveren en verwijderen (bijzondere) persoonsgegevens* [[70]](#footnote-70)[[71]](#footnote-71)[[72]](#footnote-72)[[73]](#footnote-73)
De volgende SOPdocumenten geven werknemers van SCAL richtlijnen met betrekking tot het archiveren en verwijderen van gegevens: archiveren en verwijderen van documenten en aanvraagformulieren, *zie bijlage 3E*, bewaartermijnen documenten, *zie bijlage 3F*. De SOPdocumenten geven een aantal voorwaarden voor het archiveren van o.a. resultaten van diagnostische onderzoeken en aanvraagformulieren. Het archief dient op een manier ingedeeld te zijn dat de gegevens niet verloren, beschadigd of misbruikt kunnen worden. Tevens dienen de gegevens eenvoudig te vinden zijn. Het archief is een afgesloten ruimte in de kelder van het hoofdkantoor van SCAL. Alleen de daartoe gerechtigde personen hebben toegang tot deze ruimte en documenten. Op welke wijze digitale gegevens dienen te worden gearchiveerd staat niet in een SOPdocument genoteerd. In het SOPdcument over bewaartermijnen staat per document aangegeven na welk termijn het vernietigd dient te worden. Welke motivatie achter deze termijn zit wordt niet genoemd. Zo staat er een bewaartermijn van 2 jaar vastgesteld voor de aanvraagformulieren voor een diagnostisch onderzoek. Voor de uitslagen van diagnostische onderzoeken wordt een termijn van 10 jaar opgegeven. Dit wijkt af van het wettelijke gestelde termijn van 15 jaren als men spreekt over medische gegevens.
Na verstrijken van de bewaartermijnen worden de documenten uit het archief ter vernietiging aangeboden in een speciale container. Deze container wordt opgehaald door een gecertificeerd bedrijf die de bevoegdheid heeft vertrouwelijke documenten te vernietigen.
*Datalek*[[74]](#footnote-74)[[75]](#footnote-75)Tijdens de documentenanalyse is naar voren gekomen dat SCAL nog geen protocollen heeft voor het beleid hoe men dient te handelen bij een datalek. Wel zijn er twee SOPdocumenten, *zie hiervoor bijlage 3G*, die beschrijven wat er verwacht wordt van de medewerkers bij vermissing van een buis (met bijvoorbeeld bloed van een cliënt) of juist wanneer er een buis overblijft in het laboratorium. Aangezien bloed gegevens bij zich draagt die enkel naar één persoon kan leiden zou dit kunnen worden gedefinieerd als een datalek. Er dient een formulier te worden ingevuld als er sprake is van een vermissing van een (bloed)buis. Vervolgens moet worden onderzocht of er (nog) geen bloed is geprikt bij de cliënt of dat er iets anders aan de hand is. In het SOPdocument wordt alleen nog verder ingegaan op het scenario dat men nog geen bloed heeft laten prikken. Maar hoe de medewerker dient te handelen als er daadwerkelijk sprake is van een datalek wordt niet beschreven. Als een (bloed)buis overblijft in het laboratorium dan wordt deze nog 3 dagen in de koele kamer bewaard.

***Privacyreglement Salux Healthcare leiden***
Het privacyreglement Salux healthcare Leiden is ook van toepassing bij het uitvoeren van bloedonderzoek door Scal. Het reglement is te vinden via Wikki en kan door elke werknemer van Scal gelezen worden. In dit reglement wordt de wet bescherming persoonsgegevens uitgelegd. Omdat het reglement dateert uit 2013 is het niet up to date gezien de vele (komende) veranderingen in de tussentijd.

3.3 Conclusie juridische en documentenanalyse
Aan de hand van het onderzoek naar het juridisch kader en de (beleids)documenten die gehanteerd worden binnen organisatie SCAL zijn een aantal conclusies te trekken. Middels deze conclusies zijn de interview vragen opgesteld om daarmee de praktijk te toetsen aan deze bevindingen.

 **Toestemming cliënt**
Uit de documentenanalyse komt naar voren dat SCAL het inleveren van het aanvraagformulier door cliënt voldoende acht om te spreken van toestemming voor het diagnostisch onderzoek (en mogelijk ook de bijbehorende gegevensverwerking). Echter verwacht de wet en regelgeving dat men alvorens het verwerken van persoonsgegevens mondeling of schriftelijk toestemming dient te vragen aan cliënt.
Tevens zal de toestemmingsvereiste vanaf 2018 ook schriftelijk vastgelegd moeten worden zodat SCAL kan aantonen dat er toestemming is gegeven door cliënt voor elk beoogd doel voor de verwerking van persoonsgegevens. Bij de documentenanalyse wordt niet gesproken over het vragen van toestemming aan de cliënt als men het heeft over de verwerking van persoonsgegevens.

**Informatievoorziening aan cliënt**
De informatievoorziening dient momenteel helder te zijn met betrekking tot het beoogde doel waarvoor de persoonsgegevens verwerkt worden en met wie deze gegevens gedeeld zullen worden. Indien betrokkene al op de hoogte is via een externe partner dat de gegevens gedeeld gaan worden met een andere organisatie behoeft dit niet nogmaals geverifieerd te worden. Aangezien opdrachtgever SCAL wel duidelijkheid moet hebben of de cliënt op de hoogte is van wat er met zijn (bijzondere) persoonsgegevens gebeurd kun je concluderen dat dit ten alle tijden gecontroleerd dient te worden.
De plicht om de cliënt informatie te verschaffen wordt per 2018 verscherpt. Zo dient de informatie op schriftelijke wijze worden aangeboden. Mondeling volstaat niet meer. Inhoudelijk is de informatieplicht uitgebreid. Men dient de cliënt straks ook te wijzen op de rechten van de cliënt (zoals recht op inzage, correctierecht, recht om vergeten te worden, klachtenrecht ect.), de eventuele risico’s van verwerking van zijn gegevens en bewaartermijnen van deze gegevens.
Bij de documentenanalyse is niet gebleken dat er tijdens het contact met cliënten informatie wordt gegeven over wat er gebeurd met de persoonsgegevens van hen. En welke rechten zij daarbij hebben. Op de website van SCAL wordt wel de mogelijkheid van het indienen van een klacht gemeld en welke procedure cliënt dan dient te volgen.
 **Verwerking persoonsgegevens**
Onder verwerking van persoonsgegevens wordt het verzamelen, opslaan, delen en vernietigen van deze gegevens bedoeld. Hiervoor bestaat al een aanzienlijke wet en regelgeving maar in 2018 zullen er strengere voorwaarden gaan gelden rondom het privacy beleid. Zo worden er strengere voorwaarden gesteld met betrekking tot het beschermen van de verkregen persoonsgegevens tegen misbruik, beschadiging en verlies. Ook dient men meer schriftelijke verantwoording te kunnen overleggen over welke handelingen men uitvoert om deze bescherming te kunnen waarborgen.

**Datalek**
Januari 2016 heeft Nederland het meldplicht datalekken ingevoerd in de Nationale wet en regelgeving. Dit houdt in dat SCAL een beleid moet hebben ontwikkelt om datalekken zoveel mogelijk te beperken en hoe te handelen als er toch een datalek zal voorkomen. Afhankelijk van de ernst van het datalek (hiervoor zijn criteria aangegeven) dient men de Autoriteit Persoonsgegevens in te lichten en in sommige situaties de cliënt zelf. Sprake van een datalek is als een (bijzonder) persoonsgegeven mogelijk risico loopt beschadigd te raken of als men mogelijk misbruik kan maken van een persoonsgegeven (denk aan een computerhack, virus ect.) En als men persoonsgegevens verloren of kwijt is. SCAL dient risico analyses uit te voeren om preventief te kunnen anticiperen op het gevaar van een datalek. Tevens dient er een register te zijn die de datalekken (kleine of grote) bijhoudt.
Gedurende de documentenanalyse is er geen protocol of handleiding gevonden over op welke wijze men dient te handelen bij een datalek. Wel bestaat er een protocol hoe te handelen bij vermissing van een buis en/of aanvraagformulier.

**Functionaris privacy bescherming**
Het lijkt erop dat SCAL verplicht is een privacy functionaris aan te stellen omdat zij in grote mate bijzondere persoonsgegevens verwerkt. Zo’n functionaris is gespecialiseerd op het gebied van privacy beleid binnen de sector waarin SCAL werkt. Een aanspreekpunt voor de directie en overig personeel als men vragen heeft met betrekking tot de wet en regelgeving rondom privacy beleid. Tevens zal de functionaris een rol spelen in het ontwikkelen van dit beleid en het toezien op de uitvoering daarvan.

**Hoofdstuk 4 Praktijkvoering**
Bij het onderzoek naar de praktijkvoering kwamen een aantal zaken duidelijk naar voren. Een tweetal medewerkers die ik heb gesproken (een basisanalist en een analist werkzaam op het laboratorium) kon ik enkele vragen niet stellen aangezien zij nauwelijks cliëntcontact hebben gedurende hun werkzaamheden. Hen heb ik wat die vragen betreft buiten beschouwing gelaten tijdens het opnemen van de percentages, genoteerd in de komende cirkeldiagrammen. Per vraag zal ik een korte toelichting geven. Na behandeling van de interviews met de leidinggevenden zal ik een verslag doen over de scan die ik heb uitgevoerd bij het uitvoerend personeel. Om vervolgens een eindconclusie te geven over de praktijkuitvoering met betrekking tot het privacy beleid binnen SCAL tijdens het doen van bloedonderzoek.

4.2 interviews leidinggevenden
Bij de interviews met de leidinggevenden, van informatiemanagement en IT operations (IT), laboratorium m.b.t. klinische chemie (tevens ook gedeeltelijk verantwoordelijk voor de afdeling Medical services) en laboratorium m.b.t. microbiologie, zijn een aantal vaste onderwerpen aangesneden. Per onderwerp kan de conclusie worden gelezen.
**1.Toestemmingsvereiste**Alle drie de leidinggevenden geven aan dat er geen toestemmingsvereiste geldt met betrekking tot de verwerking van persoonsgegevens. De overeenkomst wordt aangegaan met de opdrachtgever, zoals een huisarts, en niet met de cliënt zelf. Zij zien zich als een uitvoerende instantie die in opdracht van een opdrachtgever werkt. De opdrachtgever heeft een relatie met de cliënt en omdat zij de cliënt doorverwijzen dienen zij te voldoen aan de toestemmingsvereiste en niet zozeer SCAL. Tevens zou de toestemmingsvereiste de zorgplicht in het geding kunnen brengen. Er is soms sprake van een tijdsdruk ,vanwege bijvoorbeeld een ziektebeeld dat zich snel ontwikkelt, en als men dan eerst de toestemmingsvereiste moet aantonen aan diegene met wie overlegt dient te worden dan kost dat teveel tijd.
Wel geven de leidinggevenden aan dat er een mogelijkheid bestaat om bezwaar te maken tegen ander gebruik van lichaamsmateriaal of het verzoeken om de persoonsgegevens, waaronder de uitslag, niet te delen met derden (de cliënt komt dan zelf de uitslag ophalen). Deze twee opties worden niet actief aangeboden maar als de cliënt er zelf om vraagt wordt het toegepast en genoteerd.
**2. Informatieplicht**
Bij het aansnijden van het onderwerp informatieplicht komt naar voren dat de cliënt niet wordt ingelicht over de wettelijke vereiste onderwerpen. Tevens zijn er geen folders die inhoudelijk in gaan op het privacy beleid binnen organisatie SCAL of de rechten die cliënten hebben m.b.t. bescherming persoonsgegevens. Wel verwijzen de leidinggevenden naar de website van SCAL voor informatie over het klachtenbeleid, privacy beleid en ander gebruik van lichaamsmateriaal. Over deze onderwerpen staat inderdaad het één en ander genoteerd op de website.
**3. Administratieve handelingen**Uit de interviews is gebleken dat de leidinggevenden een logboek bijhouden van elke handeling die uitgevoerd wordt (ook wel ‘loggen’ genoemd). Men kan zien wanneer een onderzoek is gestart en in welk stadium het zich bevindt. Tevens wordt bijgehouden wie welke handeling uitvoert en met wie de gegevens gedeeld worden. Het logboek is alleen voor de leidinggevenden zichtbaar. Hiermee voldoet SCAL aan de vereiste om een activiteitenregister bij te houden.
Momenteel is SCAL bezig met het opstellen van bevoegdhedenlijsten waarop aangegeven staat wie waar verantwoordelijk voor is en welke handelingen men uitvoert. De leidinggevenden die ik gesproken heb zijn allen op de hoogte van deze bevoegdhedenlijst. Zij geven aan dat het duidelijk is voor hen wat de bevoegdheden zijn. Tevens geven zij aan dat ditzelfde geldt voor de werknemers waar zij leiding aan geven. Het is onderdeel van het arbeidscontract geworden.
De interviews met de leidinggevenden bevestigde dat er nog geen register voor datalekken bestaat en ook geen register voor de risico analyses op het gebied van privacy. De reden van het ontbreken van deze registers is dat er geen risico analyses omtrent privacy beleid worden uitgevoerd en een protocol voor datalekken ontbreekt. Wel geeft één van de leidinggevende aan dat het nuttig zou kunnen zijn een risico analyse uit te voeren om het privacy beleid binnen SCAL te toetsen.
**4. Datalekken**
De leidinggevenden zijn allen op de hoogte van wat gedefinieerd wordt als datalek. Wel geven zij aan dat er nog geen duidelijk protocol is, op papier, hoe men dient te handelen. Bij de vraag hoe zij zouden handelen bij constatering van een datalek geven ze allen aan zich in eerste instantie te richten tot IT. Mede om te controleren of er daadwerkelijk sprake is van een datalek maar ook om het bij hen neer te leggen zodat zij het verder kunnen op pakken. Ook wordt de kwaliteitsfunctionaris genoemd. Daar zou de melding volgens de leidinggevenden ook naar toe moeten. Welke rol de Autoriteit Persoonsgegevens in deze zou kunnen spelen wordt niet genoemd.
**5. Functionaris privacy bescherming**
Bij de vraag hoe men tegenover een mogelijke functionaris voor privacy bescherming staat wordt wisselend gereageerd. Eén leidinggevende geeft aan dat het wellicht nuttig zou kunnen zijn voor als er vragen zijn maar geeft tegelijkertijd aan dat hij zelf ook best kan nadenken en zaken op kan zoeken. Een andere leidinggevende geeft aan dat er momenteel geen prioriteit voor privacy bestaat binnen de organisatie dus dat men daar dan ook niet heel actief mee bezig is. Een zorg van de leidinggevenden is dat het aanwijzen van een functionaris geld zal kosten. Geld dat naar hun mening naar de kwaliteit van de zorg zou moeten gaan.
**6.Overig**
De leidinggevenden geven aan dat altijd geverifieerd wordt naar wie de uitslag van een onderzoek wordt verstuurd. In de regel worden geen uitslagen telefonisch gedeeld door analisten. De uitslagen dienen per fax of per een beveiligd netwerk te worden gemaild. Tevens worden steeds meer uitslagen via het beveiligd, gedeelde, netwerk zorgdomein doorgegeven. Huisartsen en andere aanvragers kunnen ook een aanvraag voor een onderzoek via dit netwerk indienen. Eén van de leidinggevende geeft aan altijd het faxnummer te verifiëren. Hij onderzoekt, alvorens de uitslag wordt gefaxt, of het nummer daadwerkelijk bij de aanvrager geregistreerd staat. Bestaat hier enige twijfel over dan wordt de uitslag niet gefaxt. Opvallend is dat het SOPdocument doorgeven uitslagen spreekt over een artsencode die gebruikt kan worden om te verifiëren wie de persoon is aan de lijn indien gebeld wordt voor een uitslag van een onderzoek. Geen enkele medewerker die gesproken is voor dit onderzoek heeft het over een artsencode gehad.
Bij de vraag hoe lang bepaalde documenten met persoonsgegevens van cliënten bewaard blijven wordt door twee leidinggevenden aangegeven dat er helemaal niets vernietigd wordt. Door de andere leidinggevende wordt een termijn van 10-15 jaar genoemd, maar helemaal zeker is hij niet. Door deze inconsistentie, die ook bij de uitgevoerde scan bij de medewerkers is geconstateerd, is het onduidelijk hoe lang bepaalde documenten gearchiveerd blijven.

4.1 SCAN uitvoerend personeel
Een aantal conclusies kunnen worden gesteld na het bestuderen van de gehouden interviews en opgemaakt scans van het uitvoerend personeel:
**1. De rechten van de cliënt met betrekking tot privacy worden niet besproken**, *zie Figuur 1*.
Eén van de vereisten voor het verwerken van persoonsgegevens is dat alvorens de verwerking de betrokkene (hierna te noemen cliënt) wordt gewezen op zijn/haar rechten met betrekking tot privacy. Met deze rechten worden een aantal zaken bedoeld: het recht om te verzoeken dat de gegevens die verwerkt zijn verwijderd worden, het recht om de gegevens in te zien en op te vragen, het klachtenrecht en recht op informatie. Het uitvoerend personeel is dan ook gevraagd of zij alvorens dat persoonsgegevens worden verwerkt zij de cliënt inlichten over zijn/haar rechten. Bij alle medewerkers, werkzaam bij de receptie en medical services, was het antwoord hierop éénduidig van niet.

**Figuur 1**

**2. Er wordt niet uitgelegd aan de cliënt om welke reden zijn/haar persoonsgegevens dienen te worden verwerkt**, *zie figuur 2*. Zo wordt bijvoorbeeld altijd het BSN nummer gecontroleerd van de cliënt. De cliënt dient zich te legitimeren alvorens het bloedonderzoek. Als men bij de receptie en soms bij de prikkamer om een legitimatiebewijs van cliënt vraagt wordt niet uitgelegd om welke reden en wat er met de gegevens gedaan wordt. Alle medewerkers gaven aan dat cliënten regelmatig zelf om de reden vragen. Dan wordt er wel uitleg gegeven over het belang en de plicht die er geldt naar de verzekeraar toe.

**Figuur 2**

**3. Er wordt geen toestemming gevraagd voor verwerking van persoonsgegevens door het uitvoerend personeel**, *zie figuur 3.*
Alvorens persoonsgegevens verwerkt worden dient de cliënt toestemming te geven voor de doeleinden waarvoor de verwerking nodig is. Doordat de cliënt al vaak het aanvraagformulier meebrengt van de verwijzende opdrachtgever (vaak een huisarts of specialist) gaat men er vanuit dat de cliënt op de hoogte is van wat er met zijn/haar persoonsgegevens gebeurd en dat ze daar dan ook mee akkoord gaan.

**Figuur 3**

**4. Er wordt geen uitleg gegeven over op welke wijze de uitslag en persoonsgegevens met de aanvrager, bijvoorbeeld de huisarts, worden gedeeld**, *zie figuur 4*. Wel geven een aantal medewerkers aan dat zij uitleggen dat de uitslag binnen een aantal werkdagen bij de huisarts ligt. Er wordt dan niet specifiek uitgelegd op welke wijze de uitslag wordt doorgegeven. Tevens geven medewerkers aan dat de cliënten de wens mogen uitspreken dat uitslagen van een onderzoek niet gedeeld worden met derden en dus ook niet met de huisarts. De cliënt komt dan zelf zijn uitslag ophalen als deze binnen is. Dit komt alleen ter sprake als de cliënt hier zelf over begint.

**Figuur 4**

**5. Er wordt niet gevraagd of de cliënt bezwaar heeft tegen ander gebruik van lichaamsmateriaa**l, *zie figuur 5*. Op het aanvraagformulier, die cliënt meebrengt als hij/zij o.a. bloedonderzoek wil laten doen, staat de vraag of de cliënt bezwaar heeft tegen ander gebruik van lichaamsmateriaal. De medewerkers van de receptie en medical services controleren wel of het vakje is aangekruist maar vragen niet actief of de cliënt bezwaar heeft. Als de cliënt uit zichzelf vraagt wat precies bedoelt wordt met die vraag dan volgt er wel een uitleg. Eén van de redenen dat de medewerkers niet vragen of de cliënt bezwaar heeft is dat het vragen oproept bij cliënten. Het beantwoorden van deze vragen kost teveel tijd en zorgt voor een langere wachttijd.

**Figuur 5**

**6. De digitale informatiebronnen zoals de SOPdocumenten in Wiki weten alle medewerkers goed te vinden**, *zie figuur 6.* Bij de vraag waar de medewerker zich tot richt als ze vragen hebben worden onder andere de SOPdocumenten die op Wiki (intranet) genoemd. Elke medewerker zegt te weten waar ze deze documenten kunnen vinden en dat het hen informatie biedt over protocollen en werkwijzen.

**Figuur 6**

**7. De digitale bronnen worden niet door iedere medewerker gebruikt**, *zie figuur 7.* Het merendeel van de medewerkers zegt de SOPdocumenten wel eens door te lezen of het te raadplegen als ze vragen hebben over werkwijzen. 20 % van de medewerkers zegt de documenten niet te lezen/gebruiken. Eén van de medewerkers geeft aan alle handelingen inmiddels wel te weten en als de medewerker toch ergens vragen over zal hebben dan ligt de voorkeur bij andere informatiebronnen zoals de leidinggevende(n).

**Figuur 7**

**8. Naast de digitale informatiebronnen geven alle medewerkers aan zich regelmatig te wenden tot leidinggevenden of collega’s**, *zie figuur 8*. Een aantal medewerkers verkiest overleg met leidinggevenden of collega’s boven het raadplegen van digitale informatiebronnen. Eén van de redenen die hiervoor wordt gegeven is dat het raadplegen van digitale bronnen meer tijd kost en men soms snel een antwoord nodig heeft. Er worden geen andere informatiebronnen genoemd die gebruikt worden bij vragen over het privacy beleid.

**Figuur 8**

**9. Alle medewerkers zijn op de hoogte van hun geheimhoudingsplicht ten behoeve van het waarborgen van privacy van de cliënten**, *zie figuur 9*. Tevens is gecontroleerd of de medewerkers ook weten wat een geheimhoudingsplicht inhoudt. Ze geven aan geen persoonsgegevens of andere informatie te mogen delen met derden, buiten de organisatie. Dit vinden zij ook een vanzelfsprekendheid en onderdeel van hun werk.

**Figuur 9**

**10. De helft van de medewerkers denkt te weten hoe lang persoonsgegevens bewaard horen te blijven, de andere helft geeft aan niet te weten hoe lang persoonsgegevens bewaard dienen te blijven**, *zie figuur 10.* Alhoewel de helft van de medewerkers zegt te weten hoe lang de persoonsgegevens worden gearchiveerd wordt er niet een éénduidig antwoord gegeven. Zo heeft iemand het over vijftien jaar en iemand anders over dat de documenten helemaal niet worden vernietigd.. Tevens geven twee medewerkers aan dat de aanvraagformulieren drie maanden worden bewaard en vervolgens vernietigd maar een andere werknemer geeft aan dat de hardcopy aanvraagformulieren veel langer gearchiveerd dienen te blijven. Uit de antwoorden kun je concluderen dat er veel onduidelijkheid bestaat over het archiveren van persoonsgegevens en uitslagen van onderzoeken. Hierdoor is geen duidelijk antwoord te geven over hoe lang de opgeslagen persoonsgegevens en de daarbij behorende uitslagen in de praktijk worden gearchiveerd.

**Figuur 10**

**11. De medewerkers geven, op één persoon na, aan niet op de hoogte te zijn van een protocol/plan als er sprake is van een datalek**, *zie figuur 10*. Het is niet duidelijk wat er van hen verwacht wordt als zij een datelek constateren. Wel geven alle medewerkers aan hoe zij denken het beste te handelen. Ze zouden allemaal direct een melding doen bij de betreffende leidinggevende.

**Figuur 11**

**12. Alle medewerkers zeggen zich voldoende bewust te zijn van de wet en regelgeving omtrent de privacy van cliënten**, *zie figuur 12*. Alle medewerkers gaven tijdens het interview aan zich bewust te zijn van de regels omtrent privacy gedurende de uitvoer van hun werkzaamheden. De gehele wet en regelgeving is voor hen niet relevant alleen het gedeelte waar zij mee te maken hebben. En dat is verwerkt in hun beleid. Of dit beleid ook daadwerkelijk voldoet aan de wet en regelgeving wordt niet in twijfel genomen. Tevens geven de medewerkers van Medical Services en Receptie aan dat zij de privacy van cliënten altijd in acht nemen. Zo houden ze cliëntgegevens altijd buiten zicht voor andere cliënten en worden documenten die niet bewaard hoeven te blijven direct in een daarvoor bestemde container geplaatst. Deze container zit op slot.

**Figuur 12**

4.3 Conclusie praktijkvoering
In dit hoofdstuk wordt antwoord gegeven op de centrale vraag:
*“In hoeverre voldoet het privacy beleid van SCAL aan de algemene verordening gegevensbescherming?”***Het toestemmingsvereiste**
Opgenomen in de Algemene verordening gegevensbescherming, is een belangrijk onderwerp. Momenteel vraagt SCAL geen toestemming voor de verwerking van persoonsgegevens als de cliënt doorverwezen wordt voor een bloedonderzoek. Er vanuit gaan dat de cliënt akkoord gaat met de verwerking van zijn/haar persoonsgegevens door het inleveren van het aanvraagformulier is niet voldoende. De medewerkers dienen alvorens het verwerken van persoonsgegevens cliënt te informeren op welke wijze hun persoonsgegevens verwerkt zullen worden en daarvoor toestemming te vragen. De toestemming dient op zo’n wijze te worden geregistreerd dat achteraf aan te tonen is dat de cliënt akkoord is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. In het bijzonder dient dit te gebeuren als het lichaamsmateriaal voor andere doeleinden gebruikt zal worden (zoals validatie van de analyse apparaten) dan waarvoor de cliënt langs kwam. Momenteel staat er een ‘opt out’ op het formulier waarbij gevraagd wordt of cliënt bezwaar heeft tegen ander gebruik van het lichaamsmateriaal. Deze vraag wordt niet actief gesteld aan de cliënten en alleen aangevinkt als de cliënt er zelf om vraagt. Met de komst van de Algemene verordening gegevensbescherming dient de cliënt actief gevraagd te worden of zijn/haar lichaamsmateriaal voor andere doeleinden gebruikt mag worden.

I**nformatieplicht**
Het informatieplicht is aangescherpt in de Algemene verordening gegevensbescherming. Momenteel wordt tijdens het cliëntencontact nauwelijks tot geen informatie gegeven over het klachtenrecht, verwerking van zijn/haar persoonsgegevens, de doeleinden waarvoor zijn/haar persoonsgegevens worden gebruikt, hoe lang de persoonsgegevens worden bewaard en wat hun rechten zijn. Een voorbeeld is de vraag aan cliënten om zich te legitimeren. Hebben zij hun legitimatie niet bij zich dan kan er geen bloedonderzoek gedaan worden. De medewerkers gaven tijdens het interview aan dat ze regelmatig vragen en commentaar krijgen op dit beleid. Pas op dat moment wordt uitleg gegeven over om welke redenen dit beleid op deze manier uitgevoerd wordt. De cliënt heeft het recht om te vragen om zijn persoonsgegevens en de uitslag van een onderzoek niet te delen met derden. Dan haalt de cliënt, na zich geïdentificeerd te hebben, zijn eigen uitslag op zonder dat de uitslag gedeeld wordt met bijvoorbeeld de huisarts. De cliënt moet dan wel zelf op de hoogte zijn van dit recht en hierom vragen. Met de komst van de Algemene verordening gegevensbescherming dient de cliënt gewezen te worden op zijn rechten met betrekking tot verwerking van persoonsgegevens. Dit kan middels folders of via de website en daar dient tevens mondeling naar verwezen te worden alvorens het bloedonderzoek wordt gedaan. Momenteel heeft SCAL geen folders over de verwerking van persoonsgegevens maar wel informatie op de website. De informatie op de website betreft het klachtenbeleid en gebruik van ander lichaamsmateriaal. Er dient nog meer informatie te worden gedeeld, hier wordt op terug gekomen bij het hoofdstuk aanbevelingen.

A**dministratieve handelingen**
Administratieve handelingen worden deels al uitgevoerd door de medewerkers van SCAL. Er bestaat een digitaal logboek waar alle handelingen die uitgevoerd worden ten behoeve voor bloedonderzoek worden genoteerd. Tevens kunnen de leidinggevenden de voortgang van het onderzoek volgen en inzien met wie en wanneer persoonsgegevens zijn gedeeld. Daarnaast voldoet SCAL aan de vereiste om een bevoegdhedenlijst bij te houden van alle medewerkers. Hierin staat genoteerd wie waar verantwoordelijk voor is. De medewerkers lijken hiervan op de hoogte.
Wat nog mist en wel een vereiste is met de komst van de Algemene verordening gegevensbescherming is een register waarin wordt bijgehouden wat de resultaten van de risico analyse omtrent privacy beleid zijn. Daarnaast dient er een register van datalekken (groot of klein) te worden bijgehouden. Deze twee registers ontbreken, mede omdat hier nog geen beleid op ontwikkelt is. Er worden geen risico analyses op het gebied van privacy gehouden en er bestaat geen duidelijk protocol over hoe te handelen bij constatering van een datalek.

**Datalek**
SCAL lijkt ver ontwikkelt als het gaat om een het hebben van een beveiligd computernetwerk. Dit is mede om de privacy van cliënten zo goed mogelijk te beschermen en dus ook datalekken te kunnen voorkomen. Onder datalekken worden niet alleen computerlekken (computerhacks, virussen ect) bedoeld maar ook het doorgeven van informatie aan de verkeerde personen, het verliezen van een bloedbuis of documenten met persoonsgegevens ect. SCAL heeft ook op dit gebied maatregelen genomen. Zo bestaat er een speciale, afgesloten, container waarin documenten met persoonsgegevens kunnen worden gedeponeerd die vernietigd moeten worden. Documenten worden buiten het zicht van andere cliënten gehouden en er wordt zo goed als het kan geverifieerd aan wie de bloeduitslagen worden doorgegeven. Tevens worden alle papieren documenten beveiligd bewaard. Alleen bevoegden hebben toegang tot deze documenten. Men lijkt zich goed bewust te zijn van het belang van privacy voor de cliënt. De medewerkers zijn er zeker van dat een datalek niet zo snel zal voorkomen binnen hun organisatie. Er bestaat geen protocol voor het geval men toch verast wordt met een datalek. Wel denkt men te weten hoe te handelen bij een datalek.

**Functionaris privacy bescherming**
De reden dat SCAL verplicht wordt voor het aanstellen van een functionaris privacy bescherming is voornamelijk omdat zij op grote schaal medische persoonsgegevens verwerkt. Momenteel is er nog geen functionaris aangewezen die toeziet op het privacy beleid. De medewerkers lijken ook niet direct de behoefte te voelen voor een duidelijk aanspreekpunt op het gebied van privacy.
Ondanks dat de medewerkers vertelden privacy van de cliënt belangrijk te vinden en daar ook naar te handelen, bleek de kennis wat betreft privacy en bescherming van persoonsgegevens op sommige vlakken onvoldoende. Zo is er onduidelijkheid over de bewaartermijnen van documenten met persoonsgegevens, weet men niet direct wat een datalek is en zijn de medewerkers niet op de hoogte van de informatieplicht en toestemmingsvereiste.

**Hoofdstuk 5 Aanbevelingen**De aanbevelingen kunnen geïnterpreteerd worden als een advies dat voortvloeit uit de bevindingen van het onderzoek. Het betreft een advies met het oog op de toekomstige algemene verordening gegevensbescherming dat vanaf het jaar 2018 volledig van kracht zal zijn. Met name omdat opdrachtgever SCAL nog tijd heeft aanpassingen in het beleid door te voeren lijkt het advies goed doorgevoerd te kunnen worden. Onderstaand de aanbevelingen.

**» Stel een functionaris privacy bescherming aan**
Mede omdat het privacy bewustzijn niet optimaal is en men privacy niet de belangrijkste prioriteit lijkt te geven is het verstandig een functionaris aan te stellen. Een persoon die privacy boven aan de lijst van de agenda plaatst en men kan wijzen op de consequenties als bepaalde zaken niet op tijd geregeld worden. Tevens zou de functionaris bepaalde onduidelijkheden over bijvoorbeeld het toestemmingsvereiste kunnen wegnemen door hier meer diepgang aan te geven middels een grondig onderzoek en overleg met bijvoorbeeld de instantie Autoriteit Persoonsgegevens.
**» Zorg voor een informatieplatform waar de cliënt naar kan worden verwezen als hij/zij een onderzoek komt laten uitvoeren.**
Het zal een toegankelijke manier van informatievoorziening moeten zijn. Denk aan folders, informatiescherm in de wachtruimte of meer informatie op de website. De onderwerpen die in ieder geval niet mogen ontbreken; welke rechten cliënten hebben, hoe lang en welke persoonsgegevens gearchiveerd worden, met wie en op welke wijze hun persoonsgegevens gedeeld worden, welke risico’s er bestaan bij verwerking van persoonsgegevens en op welke wijze deze ingeperkt worden en hoe het overig privacy beleid eruit ziet. In het bijzonder is aan te raden een uitleg te plaatsen over de legitimatieplicht alvorens een onderzoek. Hier komen regelmatig vragen over en die kunnen daarmee op eenvoudige wijze ondervangen worden. Alleen deze informatie delen op de website is niet voldoende, tijdens het cliëntencontact dient men op deze informatiebron gewezen te worden.
**»Zorg dat de toestemming van de cliënt voor de verwerking van zijn persoonsgegevens aan te tonen is op schriftelijke/digitale wijze.**
Er vanuit gaan dat de cliënt akkoord gaat met de verwerking van zijn persoonsgegevens, omdat dit bijvoorbeeld met de huisarts besproken is, is niet voldoende. Er dient aangetoond te kunnen worden dat de cliënt op de hoogte is van de wijze waarop zijn persoonsgegevens verwerkt worden en hiermee akkoord is gegaan. De verantwoordelijkheid ligt bij de organisatie waar de gegevens verwerkt worden, ongeacht welke verstandhouding er bestaat met cliënt. Op welke wijze de toestemming wordt vastgelegd is flexibel. Wel dient de toestemming mondeling of schriftelijk actief gevraagd te worden. Een optie zou kunnen zijn dat de vraag op het aanvraagformulier wordt aangevinkt bij een akkoord.
**»Zorg voor een risico analyse dat het privacy beleid van SCAL toetst en laat de resultaten hiervan vastleggen.**
Men dient een analyse te houden dat de risico’s binnen de organisatie wat betreft bescherming persoonsgegevens aan de oppervlakte legt. Vervolgens dient hierop geanticipeerd te worden en indien nodig (preventieve) maatregelen nemen. Het is belangrijk dat opdrachtgever SCAL kan aantonen dat deze analyse gehouden is en wat de eventuele vervolgstappen zullen zijn.
**»Zorg voor een protocol over de verwachte handelwijze bij constatering van een datalek en maak een register waar eventuele (kleine/grote) datalekken in genoteerd kunnen worden.** Prioriteit zou moeten liggen bij het voorkomen van datalekken. Indien er dan toch een datalek wordt geconstateerd moet iedere medewerker op de hoogte zijn hoe te handelen. Het beleid hierop dient te kunnen worden aangetoond.
**»Zorg dat alle medewerkers op de hoogte zijn van de (nieuwe) vereisten omtrent privacy beleid en hier ook naar handelt.**
De medewerkers hebben aangegeven privacy belangrijk te vinden en hier ook naar te handelen. Hier dienen zij wel duidelijke en toegankelijke handvaten voor te hebben. Zo is bijvoorbeeld het beleid rondom archiveren en vernietigen van documenten met persoonsgegevens vastgelegd. Het valt op dat de medewerkers ondanks de beschikbare documenten niet goed op de hoogte zijn van het beleid rondom het archief. De medewerkers die tijdens hun werkzaamheden in contact komen met cliënten dienen voorlichting te kunnen geven over het beleid rondom privacy. Hier moeten zij dan ook op correcte wijze over ingelicht zijn. Wellicht is het zaak om te achterhalen of de SOPdocumenten die momenteel beschikbaar zijn voor de medewerkers voldoet.
**»Leg eventueel contact met Autoriteit Persoonsgegevens voor advies rondom privacy beleid.**
De Autoriteit Persoonsgegevens (AP) heeft onder andere de taak voorlichting en advies te geven over bescherming van persoonsgegevens. Omdat er een complexiteit bestaat aangezien men met bijzondere (medische) persoonsgegevens te maken heeft zou het een mogelijkheid zijn om advies te vragen aan AP. Zij kunnen het privacy beleid beoordelen en toetsen aan de nieuwe wet- en regelgeving. Op deze manier heeft opdrachtgever SCAL alles gedaan om te voldoen aan de Algemene verordening gegevensbescherming.

**Literatuurlijst**
Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl>, Zoek op zoekwoorden; over privacy, wetten, wbp naslag, hoofdstuk 10, artikel 66 Wbp.

Autoriteit Persoonsgegevens, “De meldplicht datalekken in de wet bescherming persoonsgegevens”, 8 december 2015, bladzijde 7.

Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014.

CBP Richtsnoeren: beveiliging van persoonsgegevens, BWBR0033572, 01 januari 2016.

De gier-stam, ‘Waar gaat het heen met de Avg?’, nummer 6, augustus 2015.

Eerste kamer Kamerstuk 2015/16, 33 169, AE, bladzijde 8.

Kwaliteitshandboek Salux healthcare, versie 3, december 2015.

Kaderwet zelfstandige bestuursorganen, 2 november 2005.

Privacy reglement Salux healthcare Leiden, versie 1.0, 01 oktober 2013.

Raad van de Europese Unie, Voorstel voor een verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016.

Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, 24 oktober 1995.

Wiki, SOPMONST001, Aannemen van een aanvraag.

Wiki, SOP DOCU011, Bewaartermijnen van documenten.

Wiki, KHBB6, Bewaartermijnen documenten.

Wiki, MONST001, aannemen van een aanvraag, 2015.

Wiki, RECP008, baliewerkzaamheden, 2011.

Wiki, RECP012, zoeken in VECOZO programma, 2014.

Wiki, RAPP001, rapportage, 2015.

Wiki, DOCU002, archiveren en vernietigen van documenten, 2014.

Wiki, LIJST007, te archiveren documenten, 2011.

Wiki, KHBB6, bewaartermijnen documenten, 2014.

Wiki, ADMI007, archivering aanvraagformulieren, 2011.

Wiki, MONST009, acties na overblijven van een buis, 2013.

Wiki, MONST008, acties na missen van een buis, 2011.

Bijlagen

Bijlage 4.

Inleidende toelichting interview **Toestemming cliënt**
Uit de documentenanalyse komt naar voren dat SCAL het inleveren van het aanvraagformulier door cliënt voldoende acht om te spreken van toestemming voor het diagnostisch onderzoek (en mogelijk ook de bijbehorende gegevensverwerking). Echter verwacht de wet en regelgeving dat men alvorens het verwerken van persoonsgegevens mondeling of schriftelijk toestemming dient te vragen aan cliënt.
Tevens zal de toestemmingsvereiste vanaf 2018 ook schriftelijk vastgelegd moeten worden zodat SCAL kan aantonen dat er toestemming is gegeven door cliënt voor elk beoogd doel voor de verwerking van persoonsgegevens.

**Informatievoorziening aan cliënt**
De informatievoorziening dient momenteel helder te zijn met betrekking tot het beoogde doel waarvoor de persoonsgegevens verwerkt worden en met wie deze gegevens gedeeld zullen worden. Indien betrokkene al op de hoogte is via een externe partner dat de gegevens gedeeld gaan worden met een andere organisatie behoeft dit niet nogmaals geverifieerd te worden.
De plicht om de cliënt informatie te verschaffen wordt per 2018 verscherpt. Zo dient de informatie op schriftelijke wijze worden aangeboden. Mondeling volstaat niet meer. Inhoudelijk is de informatieplicht uitgebreid. Men dient de cliënt straks ook te wijzen op de rechten van de cliënt (zoals recht op inzage, correctierecht, recht om vergeten te worden, klachtenrecht ect.), de eventuele risico’s van verwerking van zijn gegevens en bewaartermijnen van deze gegevens.
 **Verwerking persoonsgegevens**
Onder verwerking van persoonsgegevens wordt het verzamelen, opslaan, delen en vernietigen van deze gegevens bedoeld. Hiervoor bestaat al een aanzienlijke wet en regelgeving maar in 2018 zullen er strengere voorwaarden gaan gelden rondom het privacy beleid. Zo worden er strengere voorwaarden gesteld met betrekking tot het beschermen van de verkregen persoonsgegevens tegen misbruik, beschadiging en verlies. Ook dient men meer schriftelijke verantwoording te kunnen overleggen over welke handelingen men uitvoert om deze bescherming te kunnen waarborgen.

**Datalek**
Januari 2016 heeft Nederland het meldplicht datalekken ingevoerd in de Nationale wet en regelgeving. Dit houdt in dat SCAL een beleid moet hebben ontwikkelt om datalekken zoveel mogelijk te beperken en hoe te handelen als er toch een datalek zal voorkomen. Afhankelijk van de ernst van het datalek (hiervoor zijn criteria aangegeven) dient men de Autoriteit Persoonsgegevens in te lichten en in sommige situaties de cliënt zelf. Sprake van een datalek is als een (bijzonder) persoonsgegeven mogelijk risico loopt beschadigd te raken of als men mogelijk misbruik kan maken van een persoonsgegeven (denk aan een computerhack, virus ect.) En als men persoonsgegevens verloren of kwijt is. SCAL dient risico analyses uit te voeren om preventief te kunnen anticiperen op het gevaar van een datalek. Tevens dient er een register te zijn die de datalekken (kleine of grote) bijhoudt.

**Functionaris privacy bescherming**
Het lijkt erop dat SCAL verplicht is een privacy functionaris aan te stellen omdat zij in grote mate bijzondere persoonsgegevens verwerkt. Zo’n functionaris is gespecialiseerd op het gebied van privacy beleid binnen de sector waarin SCAL werkt. Een aanspreekpunt voor de directie en overig personeel als men vragen heeft met betrekking tot de wet en regelgeving rondom privacy beleid. Tevens zal de functionaris een rol spelen in het ontwikkelen van dit beleid en het toezien op de uitvoering daarvan.

Bijlage 5A.

**Interviews leidinggevenden**

**Datum: 09-08-2016
Afdeling: Informatiemanagement en IT operations
Medewerker: Pieter Wamsteker
Functie: Leidinggevende
In dienst sinds: Vanaf november 2014

Ik heb een gedeelte van mijn interviewvragen aangepast omdat ik denk dat jullie niet veel te doen hebben met toestemming van de cliënt en de informatievoorziening.**
Daar hebben wij alles mee te maken juist.
Het functionele beheer ligt bij de afdelingen en de inrichting van systemen, die verantwoordelijkheid ligt bij ons. En als het gaat om informatiearchivatuur, daar hoort ook beveiliging bij, dan voor informatiemanagement. Dus waar we in feite mee beginnen is procesanalyses, daar passen we een ratio op toe en we geven in de matrix aan welke bevoegdheden waar liggen. Daar horen natuurlijk alle autorisaties ook bij.
**Dat is ook belangrijk in de nieuwe wetgeving inderdaad. Worden deze bevoegdheden ook vastgelegd?**
Ja. In zo’n ratio. Ik zal je dadelijk een voorbeeld laten zien.
**Wordt dat dan ook besproken met die medewerker?**
Ja, natuurlijk. Ik kan je straks een voorbeeld van een project laten zien die we nu hebben gerealiseerd voor microbiologie. Daar zijn we mee begonnen. Hoe ziet dat totale proces eruit, waar begint dat mee en waar eindigt dat mee. Het begint uiteraard met een aanvraag, die omgezet moet worden naar een order. En dan vervolgens de uitslag moet gedistribueerd worden en naar de aanvrager toe. Declaraties moeten natuurlijk gedaan worden. Het totaalproces wordt uitgeschreven en dan per processtap geven we aan wie waar verantwoordelijk is. En dan is het in één oogopslag te zien.
**Ik heb ook documentenanalyse gedaan en ik zag in het handboek wel iets over een bevoegdhedenmatrix.**
Kwaliteitshandboek, ja.
**Dus daar zijn jullie mee bezig?**
Het kwaliteitshandboek is zeg maar ontstaan vanuit het laboratorium. Daar zie je eigenlijk meer dat de fysieke stromen hebben daar meer aandacht gekregen dan de informatiestromen. En onze achtergrond is om met name te kijken naar de administratieve processen en daar hebben wij een verantwoordelijkheid. Daar waar het in ieder geval gaat om nieuwbouw of vernieuwbouw om procesanalyse te doen en die ratio’s op te zetten. Dat ga ik je dadelijk laten zien.
**Daar ben ik wel benieuwd naar.**
**En wordt die bevoegdhedenmatrix dan ook verwerkt in het arbeidscontract? Of is het iets dat los staat daarvan?**
Nou in de opzet van het project, kan ik je dadelijk ook laten zien, zorg je altijd voor dat er een brede vertegenwoordiging vanuit de organisatie is. Dat wil zeggen dat als er HR aspecten in zitten, taken kunnen veranderen, opleiding ect dan betrekken we altijd HR erin. En dat uit zich dan inderdaad soms in veranderingen in functieomschrijvingen. Taken en bevoegdheden moeten neergelegd worden maar dat ligt dan meer op de afdelingsniveau.
**Alleen jullie geven dat aan hen terug zeg maar?**
Ja, precies.
**En jullie zijn al best wel ver daarmee denk ik.**
Ja, we hebben daar behoorlijke stappen gemaakt. Er was eigenlijk helemaal niets. Laten we heel eerlijk zijn. We hadden een aantal systemen, het enige wat wij hier eigenlijk deden… we zaten eigenlijk een beetje aan de ondersteunende kant en niet de inrichtende kant. Dat is veranderd. De organisatie heeft zich gerealiseerd dat ze met IT niet verder komt en dat je informatiemanagement daadwerkelijk moet gaan inrichten. Het product dat wij leveren is uiteindelijk informatie.
**Nu ga ik even een ander stapje maken hoor. Wat mij ook opviel was het archiveren van documenten. In het handboek worden verschillende termijnen voor verscheidende documenten gehanteerd. Ik vroeg mij af in het algemeen welke documenten met persoonsgegevens, die herleidbaar zijn naar de cliënt, digitaal worden gearchiveerd?**
Je praat over documenten. Als je nog mag praten over een document is het aanvraagformulier die de aanvrager aan de cliënt mee geeft. Verder met het zorgdomein gaat alles elektronisch. Het enige wat we dan daarvan zien is het BSN en een AGB code. Het BSN dat de cliënt identificeert. Daarmee kunnen we ook alle andere benodigde informatie opvragen zoals het huisadres enzovoorts als we dat nodig hebben. En niet vergeten de verzekeringsgegevens. De AGB code identificeert de aanvrager. De aanvrager dient gemachtigd te zijn.
Nou en hoe gaat dat dan. Digitaal wordt de aanvrager gecontroleerd, daar hebben wij een module voor ontwikkelt: de controle-aanvraagmodule. En wat er wordt gecheckt is het BSN correct, hoort daar daadwerkelijk de persoon bij. Is de cliënt verzekerd. Is de AGB code correct, dus mag de aanvrager een aanvraag indienen, dat is een hele belangrijke. En dan wordt ook nog inhoudelijk de aanvraag gecontroleerd.
**En wie controleert dat dan?**
Het systeem.
**Het computersysteem?**
Ja. Op het moment dat iets niet voldoet aan de gedefinieerde uitgangspunten, komt zo’n aanvraag op een signaleringslijst. Commerce wordt daar verantwoordelijk voor, daar zal commerce nog even aan moeten wennen. Maar het zijn hun klanten, zij zijn verantwoordelijk voor een order. Dus als artsen ondersteuning nodig hebben bij het invullen van een formulier of een aanvraag via zorgdomein kunnen zij die geven en eventueel corrigeren. En als het niet te corrigeren is dan hebben we geen aanvraag.
**Oké. Want ik las ook in het handboek, ook in Wiki bij de SOPdocumenten, dat als cliënt het aanvraagformulier inlevert dat cliënt daarmee toestemming heeft gegeven. Daar wordt vanuit gegaan.**
Daar is een vakje voor dat aangevinkt kan worden. Dus de vraag moet gesteld worden van heb je bezwaar tegen gebruik van lichaamsmateriaal voor andere doeleinden.
**Oké. Maar voor het onderzoek zelf zeg maar, het laten uitvoeren en opslaan van persoonsgegevens… wordt geen toestemming gevraagd?**
Nee dat klopt.
**Zijn jullie daar wel mee bezig om dat te veranderen?**
Nee. Ik heb ook die vraag niet gekregen en dat is ook niet naar voren gekomen.
**En dat formulier, er stond ook dat als ze het inleveren dan gaan ze ook automatisch akkoord met de algemene voorwaarden. Alleen die kon ik nergens vinden.**
Dat staat niet op het aanvraagformulier volgens mij, dat ze akkoord gaan met de algemene voorwaarden. Het is natuurlijk een overeenkomst tussen enerzijds de aanvrager en SCAL. Het idiote is het gaat natuurlijk over een persoon waarover je wat gaat vast leggen. Maar de afspraken zijn op een ander niveau dan met de persoon zelf.
**Dus eigenlijk is het uitgangspunt van SCAL dat jullie een overeenkomst aan gaan met die aanvrager en dat die de verantwoordelijkheid zal moeten dragen om cliënt in te lichten.**
Ja klopt. Net zoals de uitslagen van de aanvrager gaan niet naar de persoon toe maar naar de aanvrager.
Wettelijk gezien mogen wij alleen materiaal in ontvangst nemen als wij cliënt ook kunnen identificeren.
**Zijn er termijnen vastgelegd waarbinnen de documenten dienen te worden bewaard?**
Er is een indrukwekkende verzameling want er wordt namelijk geen document weggegooid.
**Dus alles wordt bewaard?**
Alles wordt bewaard.
Dus we hebben hier in de kelder een archief staan. Terwijl op dit moment echt alles wordt gedigitaliseerd. De papieren aanvraagformulieren worden in gescand en die worden ook voor zover dat kan automatisch verwerkt. Daar hebben we dan ook een systeem voor bedacht en komt dan ook terecht in het controle-aanvraagmodule, onze gatekeeper zeg maar.
**Dat is beveiligd?**
Ja precies.
**Oké, en jullie gaan met zorgdomein werken of dat doen jullie al?**
Daar werken we al mee.
**En is dat dan het systeem waarmee jullie zaken kunnen delen met externe partners, huisartsen enzo?**Nou de huisartsen die hebben een kopje applicatie en dan een optie aanvraag digitaal indienen.
**Heeft de cliënt daar dan ook zicht in?**
Nee.
**Is het dan de huisarts die toestemming vraagt of ze de persoonsgegevens op die manier mogen delen? Wordt dat met de cliënt besproken?**
Waarschijnlijk wel maar dat weet ik niet.
De cliënt komt bij de dokter en die zegt je moet een onderzoek laten doen. Zo gaat dat…
**En is er dan wel iets van een lijst over hoe lang iets bewaard blijft? Op een gegeven moment moet het wel verwijder worden, neem ik aan?**
Wat ik al zei, de aanvragen die zitten hier in de kelder in een archief.
**Maar er is niet een termijn waarbinnen iets vernietigd moet worden?**
Ik heb hier nog niks vernietigd zien worden.
**Daar is nog niet echt een protocol voor?**
Nee. Het is een eeuwig durend archief. Dat zie je ook in de historie van het systeem want de kern van de activiteiten van SCAL was natuurlijk de biochemische laboratorium. En de volledige historie is van moment van in gebruik name tot nu staat in het Labosesysteem.
**Dat is echt wel een hele tijd.**
Dit systeem is een jaar of vijftien geleden in gebruik genomen, als het niet langer is.
**Er bestaat dus een opslag voor hardcopy documenten.**
Alles wordt ook digitaal bewaard. Dus elke formulier, praat dus maar even over formulieren. Daar wordt een scan van gemaakt en dan ontstaat er een digitale afbeelding. Die wordt bewaard zodat het altijd snel opgevraagd worden, mocht er bijvoorbeeld sprake zijn van een interpretatiefout ect.
**Maar jullie willen uiteindelijk wel af van de hardcopy bewaring?**
Ja, natuurlijk. Alleen zijn er ook handgeschreven interpretaties of opmerkingen die nog niet gelezen worden door ons computersysteem. Helaas laat in dat geval de techniek ons nog een beetje in de steek. Dat gaat gewoon nog niet goed.
**Want in principe heeft de cliënt wel het recht om te verzoeken dat een document vernietigd wordt. Is daar wel een bepaalde procedure/handleiding voor?**
Nee niet dat ik weet. Voor zover ik weet, ik heb nog nooit gehoord van een cliënt die zegt mijn gegevens moeten worden verwijderd.
**oké. Officieel hebben ze dat recht wel maar …**
Het is ook niet verstandig omdat.. wat je wil is een stukje historie opbouwen dat als iemand de volgende keer komt dat je de uitslag van het onderzoek nu kunt vergelijken met de uitslag van het onderzoek van toen. Dus vanuit die optiek is het natuurlijk raar als iemand het wil laten verwijderen.
Wat ik mij wel kan voorstellen is dat als iemand komt voor een SOAtest die wil het dan liever niet meer weten.
**Hoe gaat dat dan?**
De cliënt wordt behandeld als een niet verzekerde ook al is hij/zij dat wel. De informatie gaat dan ook niet naar een externe partij. De uitslag moeten ze zelf komen op halen en ook zelf betalen. Dus we gaan het niet versturen. De cliënt die meld zich, ik kom mijn uitslag ophalen. Die legitimeert zich en dan pas krijgen ze de uitslag mee.
**Maar het blijft wel gewoon bewaard in het systeembeheer?**
Ja. Wat in het systeem zit dat komt er niet uit, alleen in statistiek. En dat systeem is wat dat betreft potdicht.
**Jullie zijn daar denk ik ook heel erg mee bezig geweest, datalekken.** **Toch?**
Dat is algemeen bekend natuurlijk. Maar laat ik beginnen met het begin. Er was hier zeg maar een omgeving waar constant op één en dezelfde systeem, het liep best wel door elkaar heen. Dan was het voor iemand die ergens bij wilde, waar hij eigenlijk geen toestemming voor had, in het systeem met enige moeite mogelijk er bij te komen. Wat dat betreft hebben we een betere indeling, dus iedere systeem heeft daar zijn eigen compartiment in toegewezen gekregen.
**Dus een eigen toegang?**
Een eigen toegang. Dus alleen dat stukje. En de toegang tot data kan alleen via een applicatie.
De toegang tot de systemen is met username en password beveiligd. Hier op de locatie is heel veel controle want je kunt niet zomaar achter een computer zitten en iets doen. Dat hebben we ook snel in de gaten. En ga je buiten het gebouw toegang zoeken naar onze systemen moet je geautoriseerd zijn en er is nog een extra beveiliging waarbij er een code op je telefoon verschijnt. Je kent het wel, banken werken op die manier.
**Een soort tokenachtige manier?**
Precies.
**Dus in dat opzicht is het wel redelijk goed beveiligd.**
Ja. En wij vinden dat ook wel een goede manier.
**En wat betreft hardcopy documenten**?
Dat is er niet meer. Er wordt niks mee genomen.
**En de mensen die thuis werken?**
Die zijn er eigenlijk niet.
**Dus dan geldt het alleen voor huisbezoeken?**
Ja.
**En wat betreft datalekken willen ze tegenwoordig wel dat er een soort register wordt bijgehouden. Hebben jullie daar een bepaald protocol/handleiding voor?**
Nee. Daar zijn we niet mee bezig geweest.
**En worden er wel risico analyses uitgevoerd om te bekijken hoe de beveiliging van persoonsgegevens momenteel is?**
Nee, waar vooral naar wordt gekeken is de inrichting van systemen. En dan kunnen we het daarna aandacht gaan geven. Je weet, we hebben een heel klein team.
**Het kost heel veel werk.**
Het kost heel veel tijd inderdaad.
**En dan als laatste is dat er misschien een functionaris privacy moet worden ingesteld omdat SCAL heel veel medische bijzondere gegevens deelt en archiveert. Dus ik vroeg mij af, mede omdat je daar heel veel mee bezig bent, of dat je nuttig lijkt en of er behoefte aan zal zijn.**
Ik begin met het laatste, ik denk dat de behoefte door de organisatie niet wordt gevoeld. Die prioriteit heeft het wat dat betreft niet. Het nut, ja kijk, er is natuurlijk regelgeving dus je dient dat na te leven. Ik denk dat wij de zaken doen zoals we die horen te doen.
Jullie zijn al aardig ver denk ik hoor.
Dat weet ik niet, maar ik realiseer me wel dat er wat dingen anders geregeld kunnen worden. Maar ja, wat ik al zei het zou prioriteit moeten krijgen.
**Heb je zelf nog vragen over de bescherming van persoonsgegevens?**
Nee het is niet iets dat mij primair bezig houdt, moet ik heel eerlijk zeggen. Kijk, wij zijn heel hard bezig met, de portfolio is heel erg belangrijk. We ronden nu net microbiologie af, pathologie staat momenteel op de rol. We zijn al gestart met een nieuwe pilot. Dat houdt ons dan gewoon bezig.
**Dus jullie hebben je nu voornamelijk gericht op microbiologie.**
Ja.
**Dus als ik het even kort samenvat. Gaat het vooral over informatiemanagement naar de werknemers toe en het digitaliseren van de werkwijze. En niet zozeer de toestemming en informatiemanagement naar de cliënt toe. Dus eigenlijk is de cliënt wel een partij omdat het over de cliënt gaat maar de overeenkomst is met de opdrachtgever.**
Ja, precies met de aanvrager.
**Dus daar ligt eigenlijk de focus?**
Ja. We beperken ons inderdaad tot dingen die hier intern gebeuren en bij de externe partijen gebeuren. En dan houdt het gewoon op eigenlijk. Dat is de prioriteit.

**Datum: 09-08-2016
Afdeling: laboratorium (Klinische chemie)
Medewerker: Maarten Kok
Functie: Klinisch chemicus (leidinggevende en vakinhoudelijk verantwoordelijk voor medical services)
In dienst sinds: Vanaf oktober 2014**

**Je hebt net al een beetje gelezen over toestemming, dat het een speerpunt is en wat er belangrijk aan is. Er wordt geacht van de leidinggevende op de hoogte te zijn van alle regels omtrent privacy. Dus ook omtrent toestemming van cliënt. Ik begreep dat het uitgangspunt is dat er sprake is van een overeenkomst tussen SCAL en de opdrachtgever en niet zozeer met de cliënt. Ik vroeg mij af hoe jij daar in staat?**Ik denk dat het en is… je hebt ook een relatie met de cliënt. Er staat bijvoorbeeld op het formulier of men bezwaar heeft tegen gebruik lichaamsmateriaal voor wetenschappelijk onderzoek maar je hebt ook verantwoordelijkheden naar beiden toe.
**De toestemming die ik bedoel is dan vooral voor het verwerken van persoonsgegevens zoals het archiveren en delen van gegevens. Wordt dat met de cliënt besproken op één of andere manier?**
Niet direct maar we zijn wel wettelijk verplicht om het een aantal jaren te bewaren. Ik weet niet precies via welke wet maar daar staat in ieder geval in hoe lang we het moeten bewaren. En daarnaast is het ook zo dat we een contract hebben via het aanvraagformulier. We gaan er vanuit dat als je het meegeeft aan de cliënt en die komt hier dat die bewust is van het feit dat er data wordt geregistreerd.
**Je bedoelt dat het dan al besproken is met de cliënt door de huisarts?**
Ja. Dat er een laboratoriumonderzoek is aangevraagd en dat het dan ook naar die arts wordt gestuurd. Volgens mij is het met de wet zo geregeld dat data niet gedeeld mogen worden met derden maar is daarop de uitzondering als het medisch handelen daarmee in gevaar wordt gebracht. Dus dan geldt de zorgplicht die boven de wet of privacy staat.
**Dus eigenlijk komt het erop neer dat omdat ze de aanvraagformulier inleveren, dat jullie er vanuit gaan dat de cliënt op de hoogte is van wat er met hun gegevens wordt gedaan. Los van of het nog voor andere doeleinden mag worden gebruikt of niet. Dat zou dan voldoende moeten zijn als toestemming?**
Ja.
**Toestemming wordt niet ergens nog vastgelegd?**
Het is wel zo dat er een ‘opt-out’ op het formulier staat.
**Opt-out?**
Je hebt een opt-in dat je toestemming moet geven voor het onderzoek en opt-out is als men bezwaar tegen onderzoek moet maken.
Dus die mogelijkheid is er. Op papier is dat één van de vragen die moet worden ingevuld.
**En als de cliënt daar heel veel vragen over heeft dan is daar meer informatie over?**
Volgens mij staat er op de site informatie en we hadden vroeger een folder daarvoor. Ik weet niet of die er nog steeds is.
**Oké. Ik zag inderdaad op het nieuwe aanvraagformulier tussen haakjes staan ‘zie informatiefolder’.
Dan kan ik nu gelijk over gaan op de informatievoorziening voor de cliënt. Eigenlijk is mijn vraag in z’n algemeenheid wat er wordt besproken voordat het onderzoek daadwerkelijk wordt gedaan?**Dan zou je eigenlijk iemand van medical services moeten hebben. In ieder geval wordt er gecontroleerd of degene die met het aanvraagformulier komt ook diegene is die op het aanvraagformulier opgegeven staat. En vervolgens wordt de aanvraag gedaan en worden een aantal vragen doorgelopen die verplicht zijn.
**En die vragen kan ik beter aan medical services stellen?**
Ja, ik kan je ook het protocol geven. Want er is een protocol voor hoe er bloed moet worden geprikt.
**Dat staat op Wiki dan, die heb ik als het goed is al gezien.**
**Zijn er ook nog andere folders die beschikbaar zijn over bijvoorbeeld de procedure voor het indienen van een klacht ect. ?**
Er is een hele lijst met folders maar die weet ik niet uit mijn hoofd want daar werk ik niet mee. We hebben wel ook een standaardprocedure voor klachten. Zowel voor de persoon die de klacht wilt indienen als over de verwerking daarvan.
**Welke persoonsgegevens worden verwerkt bij het uitvoeren van een bloedonderzoek. Dus welke gegevens over de cliënt worden verwerkt?**
Veel. Geboortedatum, leeftijd, NAW, verzekeringsnummer…
**En de uitslag van het onderzoek.**
Ja. Het labnummer.
**En ook de verantwoordelijke van de afdeling of diegene die erop toe ziet?**
Hoe bedoel je?
**Nou de naam van de toezichthouder?**
Nee, maar de verantwoordelijkheid is wel onderverdeeld en vastgelegd. Maar niet op die manier.
**Oké. Want ik zag wel dat jullie iets doen met autorisatie?**
Ja, dat is dan wel weer vastgelegd. Dan is het wel handig om even door te spreken hoe bloedafname gaat.
In eerste instantie heb je dan de cliënt die komt met een aanvraagformulier, dan wordt geverifieerd of het inderdaad de persoon is. Vervolgens wordt dan het bloed afgenomen en wordt het materiaal dat wordt afgenomen gelabeld met een sticker met een zes cijferig-nummer. Dat wordt ook gekoppeld aan de aanvraag. En dan heb je een match tussen het materiaalnummer en het aanvraagnummer. En vervolgens komt het hier op het laboratorium, wordt het afgedraaid en gaat het naar verschillende analysers toe. Dan heb je de basisanalisten die draaien het af en die zorgen ervoor dat het monstervoorbewerking gedaan is. Daarna neemt de analist het over die zetten het in het apparaat. En dan worden de analyses uitgevoerd. Er komen getalletjes uit. Als het binnen de referentiewaarden ligt of iets daarbuiten, dat hebben we afgesteld, dan sturen ze het automatisch door. En is het sterk afwijkend dan kijkt de analist eerst nog of ze het goed gemeten hebben, zijn de controles goed uitgevoerd. En als daar uit komt dat het klopt en ze zijn sterk afwijkend dan komen ze bij mij terecht. En dan kijk ik of er meer bekend is over cliënt, is er een ziektebeeld? En op die manier kunnen we beslissen of die waarde daarbij past of dat we contact op moeten nemen met de huisarts.
**Dus eigenlijk zijn jullie niet bij elk onderzoek betrokken?**
Wel verantwoordelijk. Maar niet betrokken.
**Wel als het afwijkt.**
Ja. En er zit dus ook een stuk verantwoordelijkheid bij de analisten want die moeten hun werk ook goed doen.
**Heel veel persoonsgegevens worden tegenwoordig digitaal bewaard. Wordt er ook nog iets schriftelijk bewaard?**
Nee want wij scannen al onze formulieren in. Maar de formulieren bewaren we wel want dat zijn we ook wettelijk verplicht. Maar die gaan er geloof ik na drie tot vijf maanden ook uit. Misschien bewaren we ze langer, dat weet ik niet. Moet ik even kijken in het SOPdocument. We bewaren ze wel maar ik weet niet hoe lang.
**Oké en dan in het archief hé.**
Ja.
**Worden er bepaalde handelingen vastgelegd. Bijvoorbeeld een aftekenlijst?**
Ja, heel veel. Ook digitaal. Dat kan ik je even laten zien als je wil?
**Dat is goed. Dan zet ik het even op pauze.**
**Hoelang alles bewaard wordt dat zoeken jullie dan op als het nodig is?**
Nou dat is niet mijn taak om dat te doen maar het staat beschreven. Daar is een SOPdocument voor, ik weet dat die er is.
**Die heb ik ook gezien inderdaad.
Er is ook heel veel te doen over datalekken. Ik weet niet of je daar een beetje bekend mee bent**?
Ja, ik heb ik Alkmaar gewerkt toen ik in opleiding was en toen was er een situatie dat er echobeelden waren opgevraagd van een keeper van AZ door een arts die geen arts bleek te zijn.
**Dat was een behoorlijke datalek dan.**
Ja.
**Dat zou in principe ook hier kunnen voorkomen.**
Maar daarom hebben wij het zo min mogelijk over uitslagen. Maar natuurlijk als we het daarover gaan hebben dan wordt het wel eens lastig. Als wij actief bellen dan hebben wij telefoonnummers die wij geverifieerd hebben en die staan dan ook in Laboses. Als wij gebeld worden vragen wij om uitslagen van eerdere onderzoeken om daarmee te verifiëren of iemand beschikt over de uitslagen. Dat is dan wel het minimum wat je kunt doen, want iedereen kan wel zeggen dat hij arts is, om dat te voorkomen. En als we naar alternatieve faxnummers moeten versturen dan verifieer ik ook altijd even.
**Dus dan bel je altijd even?**
Ja, of ik kijk op internet om te achterhalen of het opgegeven faxnummer bij het ziekenhuis hoort. Want meestal geven ze aan welk ziekenhuis en welke afdeling dus dan kan je dat vrij makkelijk achterhalen.
**Mocht het toch voorkomen dat er sprake is van een datalek. Is het dan bij jou bekend welke stappen je dient te ondernemen en welke handelingen je moet verrichten?**
Nee. Ik zou dan eerst naar Pieter toe gaan om te vragen, klopt het is er een datalek? En dan is het wel ook zijn verantwoordelijkheid omdat hij gaat over de informatiemanagement. En dan ben ik meer de boodschapper dat er iets fout is gegaan.
**Wordt er wel eens een risicoanalyse gedaan?**
In ieder geval niet naar de privacy maar we hebben wel een analyse gedaan om te bekijken hoe het zit met het proces van aanvraag tot uitslag. Dat was meer van wat kan er fout gaan en niet zozeer hoe het met de privacy is gesteld.
**Zoals je al hebt kunnen lezen is er een kans dat SCAL een privacyfunctionaris moet aanstellen omdat er op grote schaal bijzondere (medische) persoonsgegevens worden verwerkt. Denk je dat het nuttig is of denk je daar hebben we eigenlijk niet zoveel behoefte aan?**Dat kan ik eigenlijk niet zeggen.
**Zou je er zelf behoefte aan hebben, dat je iemand kan aanspreken als je iets wilt weten?**Aan de ene kant zou dat wel makkelijk zijn maar ik denk dat ik ook wel goed zelf kan nadenken. En op het moment dat ik iets niet weet dan kan ik daar zelf ook wel de wet op nalezen. Tenzij ik een zwarte vlek heb. Vind ik moeilijk in te schatten. Ik denk dat het geen kwaad kan om eens te kijken of we het op dit moment allemaal goed doen. Ik weet dat de ISO waar wij ook aan mee doen wel al heel veel eisen stelt maar of dat voldoende is.
**Dat is inderdaad de vraag. En zijn er nu al specifieke vragen die je zou hebben voor zo’n iemand?**Zo’n risicoanalyse vind ik wel heel waardevol en om het daarna dan te analyseren. Is de manier zoals we nu werken de goede manier.
**Welke verantwoordelijkheden heb je zelf als het gaat om de verwerking van persoonsgegevens?**Dat is met name in mijn consultfunctie. Dus dat de data die ik doorgeef ook juist overkomt. Daar zijn wel een aantal trucjes voor zoals het laten herhalen van uitslagen. Een ander iets dat we hebben geïntroduceerd is dat er geen uitslagen door analisten worden doorgebeld maar dat er wordt gefaxt en gevraagd of de fax is doorgekomen. Dus daarmee zorg je wel dat data integer blijft. Dat heeft dan niks met privacy te maken maar met de kwaliteit.
Kijk, als er een faxnummer op het aanvraagformulier staat aangegeven dan gaan we er vanuit dat dat goed is. Maar op het moment dat dat niet het geval is en er wordt gevraagd kun je het naar een ander faxnummer zenden dan wordt dat wel gecontroleerd.
**Dan controleer je dat.**
ja.
**Nou had Pieter het over een hele mooie bevoegdhedenlijst. Heb je die zelf al eens gezien of is dat met je besproken?**
ja, er is een hele mooie bevoegdhedenlijst opgesteld.
**Dus het is wel duidelijk welke bevoegdheden en verantwoordelijkheden je hebt?**
Voor mijzelf is er op dit moment een profiel wat er ligt. En ik heb natuurlijk ook het professionele instituut waar ik aan gebonden ben dus in dat opzicht zijn mijn verantwoordelijkheden wel duidelijk. En voor de werknemers bestaat er ook een bevoegdhedenmatrix waarin staat wat ze wel en niet mogen.
**Dus dat werkt wel goed.**
Dat werkt wel goed, ja.
**En geheimhoudingsverklaring?**
Ja, ook.
**En bekwaamheidsverklaring is dat er ook?**
Dat is onder andere mijn registratie bij de NVKV. En de bekwaamheidsverklaring van de analisten zit in het dossier.
**Daar kunnen ze ook bij?**
Ja, daar is een overzicht van.
Ook nieuwe medewerkers hebben een heel programma wat ze allemaal hebben gedaan waarin uiteindelijk een paraaf door ons wordt gegeven wat betekent ‘bevoegd verklaard’.
**Dan heb ik alle antwoorden op mijn vragen. Ik weet niet of je zelf nog iets wilt weten?**
Ik vroeg mij wel af over toestemming vragen aan de cliënt of dat wel te doen is.
**Ik had het er al eerder over met Gerard en die zei ook dat het niet te handhaven is wat de wetgever vraagt. Want in principe zou voor elke handeling die gedaan wordt zou je toestemming moeten vragen aan de cliënt. Of misschien moet je het dan in de informatievoorziening naar de cliënt toe moeten verwerken. Als de cliënt komt met een aanvraagformulier zou je kunnen bespreken wat er met de gegevens gebeurd. Hoe lang de gegevens worden bewaard ect.**Staat dat in de algemene voorwaarden?
**De algemene voorwaarden kan ik niet vinden.**
Oh, dat is interessant.
**Want ik zag in het handboek van Salux zag ik wel staan dat als de cliënt het aanvraagformulier bij jullie inlevert akkoord gaat met de algemene voorwaarden. Maar vervolgens kan ik die algemene voorwaarden nergens terugvinden. Dus mijn vraag was ook of de algemene voorwaarden ergens genoteerd staan?**
Voor mij was het een vanzelfsprekendheid dat die er waren.
**Heb je op Wiki gekeken?**
Heb ik ook gekeken.
**En daar stond ook niks?**
Nee, daar kon ik het niet vinden.
**En op de website?**
Ook niet.
**Er stond wel een heel klein stukje over privacy…**
Ik kan me zo voorstellen dat het dan daar in staat.
**Nee.**
Dat je het zo kan verwoorden zoals we het ook in het handboek hebben staan. Dat de cliënt op het moment dat hij zelf de aanvraag inlevert akkoord gaat met de handelingen.
**Ja. In principe is dat een hele logische gedachte natuurlijk. Alleen is de vraag bij wie de verantwoordelijkheid ligt om uit te leggen dat het zo is. Dus op het moment dat zij het aanvraagformulier inleveren dat zij ook daadwerkelijk akkoord gaan met het verwerken van de gegevens. Dat is dan eigenlijk de vraag. Jullie uitgangspunt is vooral dat die verantwoordelijkheid bij de opdrachtgever ligt maar elke instantie die daar mee bezig is draagt een verantwoordelijkheid.**Ik ben heter wel mee eens dat de opdrachtgever primair moet uitleggen dit is jou aanvraagformulier en wat het betekent. Ik vind het wel terecht dat die plicht bij de bron moet liggen en niet bij diegene die het verwerkt.
**Als dat inderdaad zo is dan hebben jullie misschien wel de verantwoordelijkheid om te checken of het ook zo is aangekomen bij de cliënt. Is de cliënt ook echt geïnformeerd door de huisarts of niet.**
Ik denk dat je dan een onwerkbare situatie krijgt.
**Dat is een heikel punt bij wie de verantwoordelijk, die informatievoorziening en toestemming, daadwerkelijk ligt. Ik heb daar ook nog geen concreet antwoord op omdat de nieuwe wetgeving heeft het vooral over het vreemdelingenrecht en over het justitieel recht maar ze gaan niet heel diep in op de gezondheidssector waardoor het heel lastig is om daar een interpretatie op te geven. Dus ik denk dat daar eerst nog jurisprudentie over moet ontstaan.**De verantwoordelijkheid is inderdaad een lastige. De verantwoordelijkheid zou bij de opdrachtgever moeten liggen maar ook bij de cliënt. En dan is de vraag of je dat als aannemer zou moeten verifiëren. En er is dan ook nog een verantwoordelijkheid bij de mensen zelf.
**Maar dan moeten ze wel weten waar ze toestemming voor geven. Ik denk dat er best veel onwetendheid bij de cliënt zelf is.**
Dat heb je toch ook als je een telefoon koopt die je niet kan betalen. Er wordt alleen een kredietcheck gedaan. Dat doet ook iedereen. Ik denk dat het ook niet altijd even netjes gaat. De vraag is dan bij wie die verantwoordelijkheid ligt.
Ik weet niet of je hier een duidelijk antwoord op gaat krijgen.
**Nee, die ga ik denk ik ook niet krijgen. Dat zal dan één van mijn conclusies worden dat daar in ieder geval nog meer onderzoek naar moet worden gedaan zodat daar meer duidelijkheid over komt. Het is een lastig onderwerp. En ik ben benieuwd wat huisartsen hierover zullen zeggen. Die zeggen misschien ook dat de verantwoordelijkheid bij jullie ligt.**Ik denk dat de huisarts zegt, ik moet die uitslag gewoon hebben.
**Ik kan in ieder geval een aantal goede aanbevelingen doen.**

**Datum: 09-08-2016
Afdeling: laboratorium (Micro biologie)
Medewerker: Jayant Kalpoe
Functie: Microbioloog
In dienst sinds: Vanaf 2014

Ik ben bezig met het onderzoek naar privacy beleid binnen SCAL omdat er een nieuwe Europese verordening is goed gekeurd/aangenomen dat best wel veel veranderingen voor alle lidstaten met zich mee brengt. En dus ook voor Nederland. Ze willen hiermee een meer uniform beleid creëren. En dat gaat dan vooral over de vijf speerpunten die relevant zijn voor SCAL. En één van de zaken is toestemming van de cliënt. Momenteel is het al van belang dat er toestemming wordt gevraagd aan de cliënt en uitlegt wat er met zijn gegevens gaat gebeuren. Dit geldt ook voor alle andere instanties. Alleen die toestemming wordt nu verscherpt dus dat betekent dat de organisatie ook moet kunnen aantonen dat de cliënt toestemming heeft gegeven en voor welke doeleinden.**En wie is de cliënt van SCAL in dit geval?
**Diegene die bloedonderzoek komt doen.
Dus ik heb mij beperkt tot alleen het bloedonderzoek. De cliënt komt hier met een aanvraagformulier heb ik begrepen en levert die in…**
Maar nu heb je het over de patiënt. De cliënt is de opdrachtgever en wij werken in opdracht van hen. Wij voeren eigenlijk een opdracht uit van een dokter. De patiënt is dan dus eigenlijk de cliënt van de dokter. Heb je zo’n aanvraagformulier bij de hand?
**Ja, die heb ik. (pakt deze erbij). Dus jullie gaan de overeenkomst aan met de opdrachtgever en niet met de cliënt.**De dokter geeft ons de opdracht om een onderzoek te doen. De dokter heeft geadviseerd aan de cliënt, die akkoord gaat neem ik aan, om dat onderzoek te laten doen. Dus dat is denk ik een nuance. Voor ons is dus niet een patiënt.
**Dat is dan wel duidelijk maar als ik de wetgeving bekijk dan kijkt de wetgever voornamelijk naar is het een organisatie die gegevens archiveert, deelt ect of niet. Als dat het geval is, dan moet die aan bepaalde regels voldoen en één van die regels is dus die toestemming. Daar is inderdaad dan wel terecht een discussie over want wie z’n verantwoordelijkheid is het om dit te verifiëren. Is dat de opdrachtgever of diegene die het onderzoek uitvoert. En daar heb ik niet een heel duidelijk antwoord op.**Daar is wel wetgeving voor toch.
**Nou ik kon daar niet heel veel wijs uit worden. Als ik kijk naar de stukken ligt er vooral focus op het vreemdelingenbeleid en justitiebeleid, dus hoe ga je om met privacy gevoelige gegevens. Daar is heel erg op ingezoomd maar op de zorgsector eigenlijk niet.
Dat maakt het ingewikkeld, er is ook weinig jurisprudentie te vinden. Vandaar dat daar nog geen duidelijke richtlijn is. Ik dacht ik ga vooral de lijn van de verordening volgen en dan zie ik vanzelf waar ik op uit kom. En mij vooral richten op hoe jullie daar naar kijken en het in de praktijk wordt uitgevoerd. Dus daar wil ik wat vragen over stellen.**Dat is prima.
**Wat is jouw functie?**
Ik ben zelfstandig arts als microbioloog.
**Afdeling laboratorium.**
Nee gewoon voor SCAL. Eigenlijk is het meer dan alleen het laboratorium. In mijn vakgebied doe ik ook consultaties, dat zijn consulten over wat er met de patiënt aan de hand is. Dat is onderdeel van mijn taak.
**Dan is dat duidelijk.**
In principe is de privacy op dat gebied wel belangrijk want een huisarts belt mij op en die wilt weten wat het beste voor die patiënt is, zeg maar. Dus die dokter belt mij op en ik moet weten om welke persoon het gaat. Dus in dat gesprek vindt natuurlijk ook uitwisseling van patiëntengegevens.
**Precies. Dus dan moet je toch weten om wie het gaat.**
Ik kan geen advies geven als ik niet weet over welke persoon hebben we het en wat is er met de persoon aan de hand.
**En gaat het dan om het delen van een BSN nummer?**
Ik werk met name met naam en geboortedatum.
**Oké. Ik ga gewoon het rijtje met vragen af.**
**Allereerst wil ik beginnen met het vragen van toestemming aan de cliënt. Ik vroeg mij af of er toestemming wordt gevraagd voor de verwerking van de persoonsgegevens zoals bijvoorbeeld het delen en opslaan van gegevens? En op welke manier dat dan wordt gevraagd?**
Ik vraag geen toestemming aan patiënten.
**Omdat je verder in het proces zit?**
Precies ik zit verder op in het proces. Maar wat ik wel zeker weet is dat… Ik heb bij zo’n aanvraagformulier nooit een formele schriftelijke toestemming gezien. Er wordt vanuit gegaan impliciet in de interactie tussen de dokter en patiënt daar toestemming is om die gegevens te gebruiken. Anders stopt het proces. Als de patiënt zegt nee je mag mijn gegevens niet delen dan stopt daar het zorgproces. Het staat ook een beetje haaks op de hulpvraag van patiënt want waarom gaat hij naar de dokter, om geholpen te worden. Daarom gaat men er vanuit dat als je naar de dokter gaat en je hebt een hulpvraag dat je dan al toestemming geeft om de gegevens te kunnen delen en gebruiken. Anders kan niet worden voldaan aan die hulpvraag.
**Dus dat is dan het uitgangspunt?**
ja.
Als ik met een dokter overleg over een patiënt dan vraag ik niet aan die dokter dat ik eerst een schriftelijke toestemming nodig heb om te kunnen overleggen. Dat is natuurlijk niet uitvoerbaar.
**Dat is dan gelijk een goede overstap naar de informatievoorziening naar de cliënt want dan zou dat bij de huisarts moeten liggen?**
Je bedoelt dat zij moeten uitleggen wat er met hun gegevens gebeurd? Ik weet niet of dat ergens op de website staat aangegeven.
**Er staat wel iets over privacy geschreven met betrekking tot geheimhoudingsplicht ect maar niet** z**ozeer op welke wijze zaken bewaard en hoe lang gegevens bewaard blijven ect.**Ik weet wel dat er iets over gezegd wordt maar niet wat de inhoud daarvan is. Ik weet wel.. wat wilde ik zeggen… Stel iemand belt mij op, ik weet niet wie die persoon is en die zegt ik wil een uitslag opvragen. Dan is het antwoord nee. Ik moet eerst weten wie die persoon is. Dus er is wel aan die telefoon een verificatie. Ik kan zien in het systeem of de naam van de huisarts bij de patiënt hoort. En als dat niet zo is dan kan ik geen informatie geven, dat kan niet zomaar. Dan moet de patiënt schriftelijk toestemming geven. En als het goed is, is er bij de dames van de receptie daar ook een beleid voor. Dat als iemand belt om de uitslag op te vragen dat zij eerst moeten kunnen verifiëren van, is het de huisarts? Ja, dan kan de uitslag gegeven worden. Is dat niet zo dan moet er eerst een schriftelijke toestemming worden gegeven. De persoon die gemachtigd is kan de uitslag op vragen.
Het zal ook in de praktijkdocumenten van SCAL staan.
**Je bedoelt de Sopdocumenten?**
Ja. Om te voorkomen dat onbevoegden de gegevens opvragen. Volgens mij staat het niet zo uitvoerig beschreven op de website maar het is wel een beleid dat hier omschreven is en uitgevoerd moet worden.
Wat ik nog wilde vertellen, is dat in mijn contract met SCAL zit ook een geheimhoudingsverklaring. Daarin staat dat de gegevens die gegenereerd worden binnen SCAL niet gedeeld wordt en volgens mij geldt dat voor alle medewerkers binnen SCAL. Op die manier borg je natuurlijk wel dat de gegevens die je als medewerker ziet beschermd blijven.
**Maar er is niet een folder of iets dergelijks dat aan de cliënt gegeven kan worden?**
Nee maar dat is misschien wel een goed punt. Om de wetgeving te vertalen naar dit soort informatie. We moeten in ieder geval via de website communiceren naar patiënten hoe er met patiënten informatie wordt omgegaan.
**Ik las ook in het handboek dat als een cliënt het aanvraagformulier hier inlevert dan ook automatisch akkoord gaat met de algemene voorwoorden. Alleen die algemene voorwaarden, die kon ik nergens terug vinden.**
Dat is gek. Ik heb geen idee waar die zijn maar die moeten wel ergens staan.
**Het zal misschien een goed idee zijn als dat ook voor de cliënt beschikbaar zou zijn?**
Je bedoelt op de website? Ja zeker.
**Dan even een algemene vraag, welke persoonsgegevens worden verwerkt bij het uitvoeren van een bloedonderzoek?**
Er zijn een aantal dingen. Wat minimaal vereist is omdat wij de patiënt moeten kunnen identificeren is naam, geboortedatum en geslacht. Dat zijn gegevens die we in ieder geval voor de medisch inhoudelijke taken in ieder geval nodig hebben. Medische zorg is natuurlijk individueel gebonden. Daarnaast heb je ook nog een aantal wettelijke vereisten. Je moet natuurlijk voor de verzekering ook de verzekeringsgegevens hebben. Het BSN nummer is een verplichting. Dus de organisaties zullen ook vragen naar de NAW, verzekeringsgegevens en BSN nummer.
**En dan natuurlijk de uitslaggegevens die worden opgeslagen?**
Ja. Dat is ook heel belangrijk. Want hoe weet je, vijf weken later, weer kijken omdat de patiënt weer ziek is en je wilt weten hoe het ook alweer zat. Dan moet je het eenduidig kunnen terug vinden. De enige eenduidige code om het weer terug te vinden is het BSN nummer. Je kunt wel twee meneer Jansen hebben met dezelfde geboortedatum dus hoe weet je dan wie die meneer is. Dus dan heb je op z’n minst zijn BSN nummer nodig.
Dus het opslaan van gegevens via unieke identificatoren is wel heel belangrijk.
**En worden alle gegevens digitaal bewaard of ook nog hardcopy?**
Nou er is ook nog een andere wet. Volgens mij via de zorgverzekeringswet. Er is een minimale opslagtermijn voor de aanvraagformulieren en ik dacht dat het vijf jaar is, kan ook vijftien jaar zijn. Maar er is dus wettelijk gezien een minimale opslagtermijn.
**Is digitaal opslaan dan ook voldoende of zou het dan ook hardcopy bewaard moeten blijven?**
Ik heb altijd begrepen dat je ook die kopieën moet opslaan.
Nou wordt ook elektronisch veel aangevraagd.
**Via zorgdomein?**
ja. En volgens mij is het zo dat als je een papieren versie hebt dat die dan wel opgeslagen dient te worden.
**Dat is dan volgens mij wel het enige dat nog hardcopy bewaard wordt?**
Ik dacht het wel. Maar goed daar moeten ook vergrendelingen voor zijn en niet iedereen kan daar zomaar bij. Daar zijn natuurlijk ook regels voor. Er zijn natuurlijk ook wel eens ongelukken gebeurd met datalekken hé dus dat moet wel goed geregeld zijn. En dan is er natuurlijk ook nog een opslag voor bloed.
**Ja. Ik las dat er ook een speciale koelkast in het archief staat**.
Precies. En je zult ook op het aanvraagformulier de vraag hebben zien staan over wetenschappelijk onderzoek.
**Je bedoelt de vraag of ze bezwaar hebben dat hun lichaamsmateriaal gebruikt wordt voor wetenschappelijk onderzoek?**
Ja. Wetenschappelijk onderzoek is eigenlijk het minst voorkomende waarvoor we het bloed op zouden willen slaan. Neem nou een zwangere, er wordt in maand drie van de zwangerschap een bloedonderzoek gedaan. Voor de gezondheid van de moeder en kind. Of er sprake is van bepaalde infecties. Dan gebeurd heel vaak als de moeder rond de vijf maanden is en zij komt op de kinderopvang, en daar is een kindje met waterpokken. Waterpokken kan gevaarlijk zijn voor het ongeboren kind. Dan is de vraag of de moeder wel beschermd is tegen waterpokken. Als de moeder niet beschermd is moeten wij binnen 48 uur medicijnen geven aan haar om het ongeboren kind te beschermen. Wat er heel vaak gebeurd is dat we terug gaan naar het oude monster om te bekijken of zij al antistoffen in haar bloed had. Dan ga je dus terug naar het materiaal dat opgeslagen is voor een doeleinde waarvoor zij primair geen toestemming gegeven heeft. Dat is de meest voorkomende reden waarom wij het gebruiken. Vaak meer voor medische doeleinden dan wetenschappelijke. Je zou denken, welke moeder zou dat niet willen. Maar toch moet je dat expliciet vragen.
**Maar het wordt in principe dus wel standaard gedaan?**
Het opslaan van materialen bedoel je?
**Ja.**
nee, je zult zien dat hier materialen vaak maar drie dagen bewaard blijven. Dat heeft vooral te maken met opslagcapaciteit.
**Worden er ook bepaalde handelingen vastgelegd in bijvoorbeeld een computersysteem? Stel dat hier een controleur komt en die wilt alles in zien kunnen jullie dat dan overleggen?**
klopt. Maar de controleur moet eerst laten zien dat hij bevoegd is natuurlijk.
Het is ook vanuit mijn artsenberoep dat eigenlijk alles wat wij doen wordt geregistreerd.
**Als een soort activiteitenregister?**
Precies. Het is eigenlijk allemaal geautomatiseerd. Alles dat ik doe bij een patiënt wordt gelogd, zodanig dat alles te herleiden is. Iedere handeling die wordt uitgevoerd wordt onuitwisbaar gelogd.
**En wie kan dit allemaal inzien?**
Op dit moment ben alleen ik hiervoor bevoegd. Alleen de artsen zijn bevoegd dit in te zien.
In het laboratorium is dat weer anders. Daar werken ze ook met laboratoriummedewerkers. Maar die kunnen alleen hetgeen zien dat zij nodig hebben voor hun werkzaamheden.
**Staat er ook een bepaald termijn voor, hoelang dit bewaard moet blijven?**
Patiëntendossiers mag je niet vernietigen. Volgens mij staat daar een levenslange bewaartermijn op. Daar is ook een wetgeving voor.
**Ik heb zelf iets gelezen over 15 jaar?**
Dan moet je het in je eigen instelling hebben maar daarna gaat het allemaal naar archieven ect
**Zijn er nog overige maatregelen die getroffen worden om de privacy te waarborgen tijdens je werkzaamheden? Je vertelde net al over de maatregelen die getroffen worden bij telefoongesprekken…**
Ik denk dat in iedere contact en op elk niveau, met name vanuit de ICT omdat heel veel elektronisch wordt vastgelegd. De servers moeten op bepaalde manieren worden ingesteld en beveiligd. Wij werken met elektronische lijnen om bijvoorbeeld opdrachten te verzenden en te ontvangen.
**Sleutelnet bedoel je?**
Ja. Alles moet gebeuren via beveiligde lijnen. Als wij een uitslag naar de dokter sturen gaat dat ook via een beveiligde verbinding per bijvoorbeeld e-mail. De enige reden om het via beveiligde lijnen te doen is de privacy. Wij kunnen ook exact monitoren wanneer er een aanvraag bij de dokter is aangekomen, in welk stadium het zich bevindt, wanneer die is aangeleverd via het sleutelnet en wanneer sleutelnet het heeft verzonden naar de huisarts. Al die stappen kunnen we volgen.
Ik heb het wel eens gehad hoor dat iemand belde voor een uitslag maar dat was niet een gemachtigde. Dan gebeurd het ook niet. Dan verwijs ik door naar de procedure van SCAL en als je een machtiging hebt dan krijg je een kopie van SCAL.
**We hadden het net al over datalekken en daar is nu ook nieuwe wetgeving over. Volgens mij is het wel duidelijk wat een datalek in wettelijke termen is. Als een data niet goed beveiligd zijn waardoor er misbruik van gemaakt kan worden, verlies of beschadigd kan raken. Stel dat zoiets zich hier toch voordoet weet je dan welke handelingen je moet volgen? Welk protocol je dan moet volgen?**
Als er een datalek is dan ga ik naar Pieter Wamsteker (IT). Hij en de kwaliteitsfunctionaris zijn de mensen die het verder op pakken. Voor mij is het natuurlijk wel relevant maar ik kan er verder zelf niets mee doen.
**De melding moet dan in ieder geval bij hem terecht komen?**
Ja. Er moet ook wel een officiële melding gedaan worden maar ik zou eerst naar IT gaan om te vragen wat er precies aan de hand is. Maar ik denk wel dat er een procedure is dat er formeel een melding gemaakt wordt. En van daaruit gaat het lopen denk ik. Ik vraag mij wel af of ik dan de persoon ben die het zal signaleren. Wat ik wel kan opmerken is dat er iemand belt, die heeft een uitslag gekregen en ik vraag mij af of die persoon wel die uitslag mag hebben. Dan maak ik daar wel een melding van.
**Dat wordt inderdaad ook gezien als een datalek.**
Dat is dan iemand die onterecht gegevens heeft ontvangen dus daar moet een melding van gemaakt worden.
Er moet iets mee gebeuren. Het moet uitgezocht worden en de persoon die het gedaan heeft moet gecorrigeerd worden.
**En er moet dan inderdaad bekeken worden hoe schadelijk het zou kunnen zijn. En als het heel erg schadelijk is en de gevolgen zijn groot dan …**
Moet je de cliënt informeren natuurlijk.
**Ja. En dan moet ook e Autoriteit Persoonsgegevens ingeschakeld worden. Dat zijn allemaal stappen die wellicht gevolgd moeten worden. Sinds januari dit jaar zijn de regels ook aangescherpt hierop.** **Heel veel organisaties hebben het beleid daar nog niet volledig op ingericht.
Daarnaast geldt de verplichting dat er bepaalde risico analyses gedaan moeten worden om te kijken hoe het ervoor staat met de bescherming van privacy. Hebben jullie daar al mee te maken gehad?**
Ik weet het niet. Dan zou je dat aan de kwaliteitsfunctionaris moeten vragen.
**De kans is groot dat SCAL een privacy functionaris moet aanstellen binnen de organisatie. Hoe sta je daar in? Is daar een behoefte aan denk je of vind je het nuttig?**
Als het de wet is, is het de wet. Het maakt dan niet uit wat de burger denkt. Zo’n functionaris moet natuurlijk gefinancierd worden. En ik vraag mij af of de wetgever daar ook aan gedacht heeft. Als het uit het potje van SCAL betaald moet worden is het tegelijk het potje van de verzekeraar.
**Dan zal de cliënt het wellicht ook gaan merken.**
**Zijn er nu al specifieke vragen die je zou hebben voor de privacy functionaris?**
Ik vraag mij altijd af in hoeverre de patiënt er veel beter van wordt. Er is nog nooit een onderzoek geweest welke impact de privacy wetgeving heeft op de kwaliteit van de zorg voor de patiënt. Het creëert ook dillema’s voor de zorgverleners. Als iemand in het ziekenhuis ligt en een specialist belt om te overleggen dan kun je geen toestemming meer vragen. Dan zou je de wet kunnen volgen en weigeren te overleggen of je omzeild de wetgeving. Voldoe je dan aan de wet of niet?
**Dan gaat de zorgplicht als hulpverlener misschien voor de wetgeving op privacy.**
Op die manier worden wel dillema’s gecreëerd en dan hebben we het nog niet eens over de kosten. Net als alle beveiliging voor ons computernetwerk, dat kost enorm veel geld. En dat is dan alleen omdat daar een wetgeving voor is opgesteld en wij die moeten volgen. De kosten, baten analyse. Staat dat wel in verhouding met elkaar?
**Dan is de vraag of cliënten daar bij stil staan.**
Daar ben ik benieuwd naar. Als mensen echt in nood zijn dan is het ook de vraag of ze privacy nog wel belangrijk vinden.
**Er bestaat een bevoegdhedenlijst. Is dat al besproken met jou?**
Ik denk dat ik weet wat je bedoelt. Dus voor alle medewerkers bestaat er een lijst waarin wordt gemonitord welke bevoegdheden iemand heeft. Dat ligt ook bij de kwaliteitsfunctionaris. En mijn bevoegdhedenlijst is ook ergens vastgelegd.
**Dus het is duidelijk wat er van je verwacht wordt?**
Ja. En ik kan alleen de handelingen uitvoeren waar ik bevoegd voor ben.

Bijlage 5B**.

Scan uitvoerend personeel

Datum: 10-08-2016
Afdeling: Medical Services
Medewerker: Nisa Sen
Functie: Medewerker mobiele team
In dienst sinds: februari 2015**

**Kun je mij vertellen wat je hier allemaal doet? Welke handelingen ect?**
Ik krijg hier de artsen aan de lijn en assistenten aan de lijn voor inhoudelijke aanvragen over de huisbezoeken of als er eventueel nog vragen zijn over de uitslagen.
En allerlei problemen die collega’s veroorzaken zoals een gemiste buis die lossen wij verder op. Wat wij nog meer doen is collega’s op hun fouten te wijzen, dat ze moeten op letten.
**Welke fouten?**
Nou bijvoorbeeld bij vermiste buizen, of ze hebben iets verkeerd gestickerd dan wijzen wij hen daar op. We krijgen eigenlijk een beetje alles binnen hier.
**Dus jullie controleren ook de aanvragen die binnen komen?**
Ook inderdaad. De faxen komen hier binnen en dan voornamelijk van huisbezoeken. We maken ook de planning voor de huisbezoeken en we maken de routes daarvoor klaar. Dat is eigenlijk een beetje wat wij hier doen.
**Dat is best veel.**
**Ik richt mij vooral op het bloedonderzoek en dan de privacy die daarbij hoort. Heb je veel te maken met privacy?**
Op zich wel. Want bijvoorbeeld van de week hebben we een probleem gehad dat we hier een cliënt hebben gehad waar we een buis van missen. En we hadden alleen het telefoonnummer van haar vader. En ik kan niet de vader bellen van uw dochter is hier geweest voor een bloedafname. Dus dat ging een beetje heen en weer maar dat is opgelost. We hebben uiteindelijk een brief naar het adres verstuurd.
**En dan ter attentie van haar?**
Ja, precies.
**En als een arts of assistente belt neem je dan ook nog maatregelen om te controleren wie je aan de telefoon hebt?**
Als artsen bellen dan benoemen ze het eigenlijk wel van ik ben die huisarts. En je hoort het ook aan de stem. Als je hier een tijdje hebt gewerkt dan herken je het natuurlijk wel. We controleer nog wel af en toe de patiëntgegevens om te kijken of het overeenkomt. En dan vragen we ook altijd naar de achternaam en geboortedatum want anders kan ik natuurlijk ook niks opzoeken.
**Bellen cliënten zelf wel eens?**Ook wel eens maar dat is dan meer om te vragen of ze op de lijst staan. Of iemand vandaag bij hen thuis komt.
**Niet voor de uitslag?**
Nee dat niet. Dat gaat via de huisarts.
**Ik heb vragen over of er bijvoorbeeld toestemming wordt gevraagd aan de cliënt maar daar heb je verder niets mee te maken of wel?**
Nou qua toestemming is het meestal vooraf. Ze hebben inderdaad de mogelijkheid om te zeggen ik geef geen toestemming dat gegevens aan derden worden uitgegeven. Maar dat is echt aan het begin dat dat aangegeven moet worden.
**En is dat bij de receptie dat het aangegeven wordt?**
Nee dat is bij het prikken zelf.
**Oké. En bedoel je dan over het gebruik van lichaamsmateriaal voor andere doeleinden?**
Ook en ook voor de uitslagen.
**En dat vragen jullie dan aan de cliënt?**
Dat moeten ze eigenlijk zelf aangeven. Dat ze dat zelf willen ontvangen.
**En op het moment dat ze dat aangeven wordt het dan nog ergens genoteerd?**
Ja, we werken met het zorgdomeinsysteem en dan heb je inderdaad rechts onderin een vakje dat aangekruist kan worden als cliënt bezwaar heeft voor gebruik van lichaamsmateriaal anders dan het bloedonderzoek.
**En ook voor delen met derden?**
Dat weet ik niet zeker.
**Hebben jullie ook een mogelijkheid om notities te maken bij de aanvraag?**
Ja.
En vaak als bijvoorbeeld een ziekenhuis gegevens van een patiënt nodig heeft dan krijgen we meestal automatisch een ondertekent toestemmingsformulier meegestuurd.
**Mocht je nou hier op werk denken van ik weet het even niet of hoe zat het ook alweer met die regels of werkwijze, waar ga je dan naar toe?**
Als mijn teamleider aanwezig is ga ik gewoon naar haar toe. Als zij er niet is dan ga ik naar de klinisch chemicus toe.
**Gebruik je wel eens computerbronnen of andere documenten als er vragen zijn?**
We hebben ook onze eigen Wikisysteem daar hebben we zeg maar alle Sops. Als je antwoorden nodig hebt voor vragen die je hebt dan staan die daar ook op. Ik persoonlijk gebruik het niet zo heel vaak en als ik mij af vraag hoe zat dat ook alweer, meestal zijn het ook vragen waar ik dan snel antwoord op moet krijgen, dus dan kan ik het beter gaan vragen.
**Heb je wel eens vragen over privacy of is dat voor jou allemaal wel duidelijk?**
Nee eigenlijk niet. Alleen laatst die situatie met de telefoonnummer van die vader want ik had helemaal geen ander telefoonnummer van dat meisje.. was ik wel aan het twijfelen van moet ik die vader nou wel of niet gaan bellen. En toen ben ik dus wel gaan overleggen met de klinisch chemicus.
**Dan weet je dus wel naar wie je toe moet en wat je moet doen.**
Precies.
**En gebruik je ook nog protocollen, handboeken, checklisten of andere bronnen?**
Nee alleen de digitale bronnen.
**En als het gaat om je werk en alle gegevens die je ziet. Heb je dan ook een geheimhoudingsplicht?**
We hebben wel een geheimhoudingsplicht, ja. Je kan niet vertellen van nou die meneer is hier geweest voor bloedafname. Dus we hebben wel een geheimhoudingsplicht.
**Weet je toevallig ook hoe lang alles bewaard wordt van wat er in de computer wordt gezet?**
Er worden eigenlijk alleen uitslagen in gezet en niet zozeer de gegevens van patiënten. Het is meer vooral de bloeduitslagen en overige uitslagen en die worden eigenlijk best wel lang bewaard. Gewoon hoe lang ze in het systeem kunnen blijven.
**Want het aanvraagformulier wordt ook ingescand toch?**
Die wordt inderdaad ingescand en kunnen we terugkijken tot een bepaalde periode. Dat is vaak echt een paar weken. En als ik het niet meer terug kan vinden in de scan dan ga ik gewoon naar het archief toe.
**Het archief is voor de hardcopy, de papieren versie?**
Ja. Dat zijn echt alleen papieren versies en die worden dan bewaard in het archief.
**Dus als je het niet in de computer kan vinden omdat het maar tijdelijk beschikbaar is dan ga je naar het archief?**
Ja.
**Ben je een beetje op de hoogte van alle privacy regels enzovoorts?**
Ik neem aan van wel.
**Hier in het bedrijf in ieder geval wel?**
Ja, dat denk ik wel. Het belangrijkste is natuurlijk de geheimhoudingsplicht en dat je inderdaad de uitslagen van iemand niet zomaar mag delen met andere personen. Dat lijkt mij wel één van de belangrijkste dingen.
**Is het ook. En is er nog overige informatie dat gedeeld wordt met de cliënt over wat er met hun gegevens gebeurd?**
Nee, eigenlijk niet. Het is gewoon iemand komt langs, laat bloed afnemen en klaar volgende patiënt.
**Dus het enige dat gevraagd wordt is of ze bezwaar hebben tegen gebruik van lichaamsmateriaal voor andere doeleinden?**
Het is eigenlijk zo dat die vraag niet wordt gesteld maar dat ze het zelf aan kunnen geven. Want wij vragen daar niet naar omdat we te maken hebben met wachttijden. Als je die vraag wel stelt dan gaat de patiënt ook meer vragen stellen over wat er precies mee gedaan wordt ect en dat is dan eigenlijk niet te doen dan. Het duurt dan alleen maar langer als je al met een volle wachtkamer zit. Maar als de cliënt het zelf aangeeft dan wel.
**En voor de rest wordt het BSN nummer opgevraagd en gecontroleerd toch?**
We controleren het legitimatiebewijs en eventueel het zorgverzekeringspasje. Maar eigenlijk doen we vooral het legitimatiebewijs controleren.
**Of het de persoon is die aangegeven staat op het aanvraagformulier?**
Ja, precies. En er wordt altijd gekeken naar het BSN nummer, achternaam en geboortedatum.
**En leg je dat dan ook uit aan de cliënt waarom je dat controleert?**
Nee, het moet gewoon. We moeten gewoon zeker zijn dat het de juiste patiënt is. Vaak als mensen inderdaad zeggen van moet dat weer of moet ik het echt laten zien, dan geef ik wel aan dat ik zeker moet zijn dat hij/zij de juiste persoon is. Dan geef ik dat wel aan ja.
**Gebeurt dat vaak dat mensen daar opmerkingen over maken?**
Best wel vaak. Heel vaak.
**Oké. En zijn dat dan mensen die hier vaker komen of mensen die hier één keer komen voor een onderzoek?**
Dat is wisselend. Er zijn er een aantal die hier inderdaad regelmatig komen en zeggen van moet dat nou weer. En je hebt mensen die zeggen van ik heb het nou echt niet bij me maar kun je me niet gewoon prikken.

SCAN medewerker: Nisa Sen

|  |  |  |
| --- | --- | --- |
|  | Ja/Nee | Toelichting |
| 1. Wordt de cliënt gewezen op zijn rechten(recht om vergeten te worden, inzagerecht ect.) met betrekking tot privacy bij zijn/haar contact met de betreffende medewerker?  | Nee |  |
| 2. Wordt aan de cliënt uitgelegd om welke reden de persoonsgegevens (zoals BSN nummer) dienen te worden verwerkt? | Nee | Mits de cliënt er een opmerking over plaatst of onvrede uit |
| 3. Wordt er toestemming gevraagd voor verwerking van persoonsgegevens aan de cliënt? | Nee |  |
| 4. Indien ja, wordt deze toestemming schriftelijk vastgelegd? | - |  |
| 7. Wordt aan de cliënt uitgelegd op welke wijze zijn/haar persoonsgegevens gedeeld worden met de opdrachtgever (bijv. huisarts)?  | Nee | Wel kunnen ze zelf aangeven dat ze niet willen dat de uitslag aan derden wordt verstrekt |
| 8. Wordt aan de cliënt gevraagd of hij/zij bezwaar heeft tegen ander gebruik lichaamsmateriaal? | Nee | Cliënt dient het zelf aan te geven.Kost teveel tijd omdat er vragen opgeroepen worden door de vraag aan cliënt te stellen. Dan neemt de wachttijd toe.  |
| 9. Welke bronnen gebruikt u voor het uitvoeren van handelingen die bij het doen van onderzoek horen? | n.v.t. | Wiki (Sopdocumenten) en de leidinggevende(n) |
| 10. Zijn er nog andere manieren om aan informatie te komen als er vragen zijn over privacy beleid? (checklisten, protocollen ect.)  | Nee | Alleen de digitale bronnen |
| 11. Als het gaat om bedrijfsgegevens heeft u dan een geheimhoudingsplicht?  | Ja |  |
| 12. Weet u hoe lang persoonsgegevens dienen te worden bewaard?  | Ja | Hoelang ze in het systeem bewaard kunnen blijven |
| 13. Bent u op de hoogte van de maatregelen die getroffen dienen te worden als er sprake is van een datalek? | Ja |  |
| 14. Bent u zich bewust van de wet- en regelgeving op het gebied van de privacy van cliënten?  | Ja |  |

**Datum: 10-08-2016
Afdeling: Medical Services
Medewerker: Liesbeth Eduards
Functie: Doktersassistent
In dienst sinds: 2009

Ik heb al begrepen dat je met name bloed prikt bij mensen. Kun je mij vertellen hoe dat dan gaat?
De cliënt komt binnen met een aanvraagformulier…**Ik haal ze uit de wachtkamer, ik stel mij voor, ik wijs ze waar ze hun jas kunnen ophangen en waar ze kunnen zitten. Dan kijk ik of ze een formulier bij zich hebben, soms hebben ze die niet. Ik controleer dan hun gegevens op het formulier. En als er geen formulier is dan kan ik met legitimatie en verzekeringsbewijs op zoeken. Ik controleer ook de legitimatie en verzekeringsbewijs. Als de receptie dat niet al gedaan heeft.
Dus de receptie doet dat soms al voor jullie?
Ja. Als het niet gedaan is dan doe ik het en als het wel al gedaan is dan noem ik ze nog eens bij hun naam en vraag ik de geboortedatum om te controleren omdat ik ga prikken. En dan plak ik een barcode/sticker op het formulier, ik kijk wat ik moet prikken en ik selecteer de buizen. En ik stel vragen die erbij horen wat het onderzoek betreft. En dan leg ik uit wat ik ga doen. Als het de eerste keer is dat iemand geprikt wordt dan zal ik meer uitleggen. En dan ga ik prikken.
**En op het moment dat je de gegevens controleert van diegene, leg je dan ook uit waarom je dat doet?**
Als het iemand is die er een opmerking over maakt dan leg ik het wel uit. Dat het belangrijk is en dat het een wet is en een regel is in dit bedrijf dat het wordt gecontroleerd. En dat het goed is voor de patiënt en voor ons zodat we de uitslag snel en goed kunnen doorgeven.
**Krijg je vaak opmerkingen erover, dat jullie om de legitimatie vragen? Of valt dat wel mee?**
Dit jaar minder. Ik werk hier al een aantal jaar. De eerste jaren wel. En als je het dan uitlegt dan draaien ze wel bij. Maar dit jaar vind ik echt dat mensen goed hun legitimatie en verzekeringsbewijs meenemen. En sommige mensen, ja, een kleine deel. We krijgen minder opmerkingen.
Afgelopen maandag hadden we iemand die vond het wel moeilijk omdat hij zijn pasje niet bij zich had. Ik kon het toen wel oplossen met het opzoeken van de verzekeringsmaatschappij. Maar soms reageren mensen wel van waarom moet dat, ik heb het de vorige keer toch al laten zien. Dan hoeft het toch niet meer. Dan leg ik ook uit van sommige zaken kunnen veranderen, zoals adres ect En dat leg ik dan ook uit en dan draaien ze wel bij.
**Dat het ook in hun belang is.**
Ja.
**Wordt er dan nog verder iets uitgelegd tijdens die handelingen? O ver privacy of gegevens die opgeslagen worden ect**
Nee niet zozeer.
**Meer over het onderzoek zelf?**
Over het onderzoek zelf. En als ze een formulier hebben dan staat daar wel over of ze bezwaar hebben tegen het gebruik van lichaamsmateriaal voor wetenschappelijk onderzoek. Maar dat ga ik niet uitgebreid uitleggen, nee.
**Vraag je dat wel, of ze er bezwaar tegen hebben.**
Dat moeten ze zelf aangeven. Dat vraag ik niet, daar ben ik eerlijk in.
**En als ze er zelf mee komen, dat ze er zelf vragen over stellen. Heb je dat wel eens meegemaakt?**
Nee, niemand vraagt daarover. Wel is er soms dat het lab vraagt of een monster gebruikt mag worden om een apparaat te testen. En dan vraag je toestemming om nog een extra buis af te nemen om het apparaat te controleren. En ze hebben geen bezwaar hoor, iedereen doet mee. Ze vinden van, het is voor een goed doel en belangrijk voor de gang van zaken hier. Maar het gaat wel om privacy maar ze doen het wel.

**Wordt er ook nog uitgelegd aan cliënt op welke manier de uitslag doorgegeven wordt?**
Aan de huisarts. Ik ga niet uitleggen op welke manier. Wat ik dan wel, en iedereen doet dat want dat hebben ze ons geleerd en dat nemen we in acht, dat als ik klaar ben met de patiënt zijn gegevens ik het formulier opberg met de kant waar geen gegevens op aangegeven staan. Dat wordt in acht genomen voor de privacy. Want je kunt daar anders zitten en alles lezen van de vorige patiënt. Ook de andere dingen zijn weg uit het zicht van de andere patiënt. Dus dat wel. Daar houden wij rekening mee maar dat weten zij niet.
**Maar jullie houden daar wel rekening mee als het gaat om privacy.**
Ja. En je zit ook apart dus je kunt vrijuit praten.
**Mocht je denken van ik heb vragen over privacy of hoe je moet handelen in bepaalde situaties, wat doe je dan?**
Dan ga ik naar de leidinggevende. Op dit moment kan mij niks te binnen schieten met wat maar als er wat is dan zou ik dat doen. Er komt altijd wel een oplossing voor.
**Zijn er nog andere bronnen die je gebruikt? Misschien iets op internet of op de computer?**
Voor privacy?
**Ja.**
Gewoon de richtlijnen, de Sops.
**Lees je die wel eens?**
Ja, ik werk veel dus die gebruik ik vaak. Gisteren heb ik er nog in gelezen.
En als ik weet dat ik een nieuw persoon heb om in te werken dan ga ik het weer opnieuw lezen.
**Heb je ook een geheimhoudingsplicht?**
Ja.
**Weet je ook hoe lang de gegevens die je invoert bewaard blijven?**
Nee, dat weet ik niet.
**Stel dat er iets gebeurd, dat er toch gegevens aan de verkeerde persoon is doorgegeven of dat er iets verloren gaat zoals een buisje bloed of aanvraagformulier, weet je dan ook wat je moet doen?**
Daar is een protocol voor. Maar dat gebeurd niet veel bij mij want ik vervoer het naar het laboratorium en daar zal het misschien wel gebeuren. Maar dan is er een stappenplan. Alles is verpakt in Sops. Alle handelingen zijn verpakt in procedures en de regels daarover zijn duidelijk.
**En dan kun je in Wiki kijken, wat moet ik nu doen?**
Ja.
**Ben je een beetje bezig met privacy of zeg je van ik doe gewoon mijn werk?**
Ik ben zeker wel bezig met privacy. Ik zorg ervoor dat ik één persoon helemaal klaar heb en als de volgende patiënt binnen komt dan zorg ik dat er niks meer ligt van de vorige. Alles buiten zicht. Ik ben mij bewust, en ik denk dat de anderen dat ook doen. Ook werk ik heel veel mensen in. Het is mij helder. Ik ben mij er super van bewust. Ik wil soms privacy dus dan geef ik dat ook. Bij dit beroep hebben we met gegevens van personen te maken die misschien elders terecht kunnen komen dus dan moet je privacy heel hoog houden.
**Hartstikke goed.**

SCAN medewerker: Liesbeth Eduards

|  |  |  |
| --- | --- | --- |
|  | Ja/Nee | Toelichting |
| 1. Wordt de cliënt gewezen op zijn rechten(recht om vergeten te worden, inzagerecht ect.) met betrekking tot privacy bij zijn/haar contact met de betreffende medewerker?  | Nee |  |
| 2. Wordt aan de cliënt uitgelegd om welke reden de persoonsgegevens (zoals BSN nummer) dienen te worden verwerkt? | Nee | Mits de cliënt er zelf een opmerking over maakt of er onvrede over uit |
| 3. Wordt er toestemming gevraagd voor verwerking van persoonsgegevens aan de cliënt? | Nee |  |
| 4. Indien ja, wordt deze toestemming schriftelijk vastgelegd? | - |  |
| 7. Wordt aan de cliënt uitgelegd op welke wijze zijn/haar persoonsgegevens gedeeld worden met de opdrachtgever (bijv. huisarts)?  | Nee |  |
| 8. Wordt aan de cliënt gevraagd of hij/zij bezwaar heeft tegen ander gebruik lichaamsmateriaal? | Nee | Cliënt dient het zelf aan te geven |
| 9. Welke bronnen gebruikt u voor het uitvoeren van handelingen die bij het doen van onderzoek horen? | n.v.t. | Wiki (Sopdocumenten) en de leidinggevende(n) |
| 10. Zijn er nog andere manieren om aan informatie te komen als er vragen zijn over privacy beleid? (checklisten, protocollen ect.)  | Nee | Alleen de digitale bronnen en leidinggevende(n) |
| 11. Als het gaat om bedrijfsgegevens heeft u dan een geheimhoudingsplicht?  | Ja |  |
| 12. Weet u hoe lang persoonsgegevens dienen te worden bewaard?  | Nee |  |
| 13. Bent u op de hoogte van de maatregelen die getroffen dienen te worden als er sprake is van een datalek? | Nee | Wel weet ik dat er een richtlijn voor bestaat en waar ik die kan vinden |
| 14. Bent u zich bewust van de wet- en regelgeving op het gebied van de privacy van cliënten?  | Ja |  |

**Datum: 10-08-2016
Afdeling: Medical Services
Medewerker: Lisa Okrouhlik
Functie: Medewerker basic medical services
In dienst sinds: September 2015

Kun je vertellen welke handelingen je uitvoert? Ik richt mij voornamelijk op het bloedonderzoek en de persoonsgegevens die daarbij worden verwerkt. Kun je mij beschrijven, er komt iemand binnen met een aanvraagformulier wat doe je dan?**Ik haal de patiënt opuit de wachtkamer en dan heb je natuurlijk een formulier met informatie. Even denken, wat doe je dan…
In principe doe ik altijd de deur dicht als ik ga prikken en dan zit je met één patiënt in de prikruimte. Als het goed is het dan privé. Soms lopen er dan nog wel collega’s binnen maar dat blijft natuurlijk gewoon onder de werknemers. Vervolgens als je dan geprikt hebt, het bloed is anoniem want het is met een barcode. De papieren zetten we dan neer dat als er nieuwe patiënten binnen komen dat niet kunnen zien.
**Ik hoorde van je collega, ze komen dan met een aanvraagformulier, dat je dan ook moet controleren of de persoon klopt met wat er op het formulier aangegeven staat?**
Ja, dat klopt. Tegenwoordig wordt dat bij de balie al gedaan. Vroeger deden we dat altijd zelf maar op deze locatie vragen ze bij de receptie al om een legitimatiebewijs voor het verzekeringsbeleid.
**Dus dat doe jij niet?**
Ondertussen heb ik vernomen dat dat niet meer gecontroleerd hoeft te worden. Ik doe het eigenlijk niet altijd meer. Soms vraag ik wel eens de geboortedatum.
**Soms?**
Ja, niet altijd. Ik ben er een beetje inconsistent mee.
**Leg je dan ook nog uit wat er verder gaat gebeuren met de uitslag en gegevens?**
Ik zeg altijd standaard dat de uitslag binnen twee dagen bij de huisarts ligt. We hebben het verder niet over wat er gebeurd met het bloed. Als mensen er naar vragen dan zeg ik altijd dat het binnen het bedrijf blijft. Het wordt alleen verzonden naar de aanvrager van het onderzoek, zoals een huisarts en verder niet aan anderen.
**Maar vertel je dat ook of leg je dat alleen uit als ze er naar vragen?**
Nee, alleen als ze er naar vragen.
**Wordt er gevraagd of de cliënt bezwaar heeft tegen het gebruik van lichaamsmateriaal voor wetenschappelijk onderzoek?**
Nee, eigenlijk niet.
**Het is wel een optie op het aanvraagformulier dus jullie kijken wel of het aangevinkt is?**
Ja, we hebben die specifieke vraag inderdaad op het aanvraagformulier staan. Ik heb doorgekregen dat we het niet hoeven te vragen.
**Zijn er nog andere zaken waar je rekening mee houdt als het gaat om privacy?**
Nou, we hadden wel eens kamers waar je met twee patiënten tegelijk zit. Dat vond ik niet zo netjes. Maar dat was alleen als het heel druk was en in principe, ik denk niet dat het nog veel gebeurd.
Ik probeer altijd netjes de deur gesloten te houden en dat er geen gegevens van andere patiënten te lezen is.
**Heb je ook een geheimhoudingsplicht?**
Ja.
**En stel je komt iets tegen op het gebied van privacy en je weet niet goed wat je er mee moet doen heb je dan bepaalde bronnen waar je naar toe gaat?**
Ik ga altijd naar collega’s om te overleggen.
**En gebruik je ook internet of een handboek dat jullie misschien hebben liggen?**
Je bedoelt op het gebied van privacy?
Ja. Daar hebben we richtlijnen voor die je kan terug vinden. Niet dat ik ze heel veel gebruik.
**En waar staan die richtlijnen dan?**
Op Wiki via de Sops.
**Mocht er nou toch iets per ongeluk kwijt raken of er zijn gegevens ergens terecht gekomen waar ze niet horen, weet je dan ook wat je zou moeten doen?**
Ik zou naar mijn collega’s gaan en die hebben daar meestal een eenduidig antwoord op. Ik heb wel eens een situatie gehad dat er een formulier was blijven liggen maar dat ligt in principe dan gewoon naar beneden zodat niemand het kan lezen. En dan ga ik naar hen toe dat er iets is fout gegaan en wat ik daarmee moet doen.
**Dus er is altijd wel iemand die jou dan kan helpen?**
Ja. Ik vraag de dingen altijd na.
**De gegevens die je in voert, weet jij hoe lang dat ongeveer bewaard blijft?**
Geen idee.
**Houd je je bezig met privacy, ben je daar bewust mee bezig?**
Nou ja, in het begin toen ik hier net kwam werken was ik er wel mee bezig. Dat je soms de neiging had van oh, ik heb een bekende gezien en dan moest ik daar wel over nadenken dat ik dat niet kan vertellen. En verder heb ik wel eens, in de zomer, dan hebben we wel eens prikkamers waar geen airco is en dat het er ontzettend heet kan worden. En dan gaat de deur open. Dat vind ik zelf meestal niet zo netjes dus dat probeer ik dan niet te doen.
**Heb je zelf nog vragen aan mij?**
Nee.

SCAN medewerker: Lisa Okrouhlik

|  |  |  |
| --- | --- | --- |
|  | Ja/Nee | Toelichting |
| 1. Wordt de cliënt gewezen op zijn rechten(recht om vergeten te worden, inzagerecht ect.) met betrekking tot privacy bij zijn/haar contact met de betreffende medewerker?  | Nee |  |
| 2. Wordt aan de cliënt uitgelegd om welke reden de persoonsgegevens (zoals BSN nummer) dienen te worden verwerkt? | Nee |  |
| 3. Wordt er toestemming gevraagd voor verwerking van persoonsgegevens aan de cliënt? | Nee |  |
| 4. Indien ja, wordt deze toestemming schriftelijk vastgelegd? | - |  |
| 7. Wordt aan de cliënt uitgelegd op welke wijze zijn/haar persoonsgegevens gedeeld worden met de opdrachtgever (bijv. huisarts)?  | Nee |  |
| 8. Wordt aan de cliënt gevraagd of hij/zij bezwaar heeft tegen ander gebruik lichaamsmateriaal? | Nee | Cliënt dient het zelf aan te geven |
| 9. Welke bronnen gebruikt u voor het uitvoeren van handelingen die bij het doen van onderzoek horen? | n.v.t. | Wiki (Sopdocumenten) en d.m.v. overleg met collega’s |
| 10. Zijn er nog andere manieren om aan informatie te komen als er vragen zijn over privacy beleid? (checklisten, protocollen ect.)  | Nee | Alleen de digitale bronnen en overleg met collega’s |
| 11. Als het gaat om bedrijfsgegevens heeft u dan een geheimhoudingsplicht?  | Ja |  |
| 12. Weet u hoe lang persoonsgegevens dienen te worden bewaard?  | Nee |  |
| 13. Bent u op de hoogte van de maatregelen die getroffen dienen te worden als er sprake is van een datalek? | Nee | Ik zou wel naar mijn collega’s gaan |
| 14. Bent u zich bewust van de wet- en regelgeving op het gebied van de privacy van cliënten?  | Ja |  |

**Datum: 10-08-2016
Afdeling: Receptie
Medewerker: Carolien
Functie: Baliemedewerkster
In dienst sinds: 2005

Ik heb een aantal korte vragen over hoe jullie te werk gaan. Ik heb vanmorgen al mensen van de prikdienst gesproken en zij gaven aan dat de cliënt zich bij de balie dient aan te melden met een aanvraagformulier. En dat er dan om een legitimatiebewijs gevraagd wordt?**Ja, klopt. **Waar is dat precies voor?**Er worden gaandeweg, ook door de assistentes, fouten gemaakt. Cliënten met een heel verkeerd formulier, geboortedatum die niet kloppen. En een BSN nummer is een BSN nummer. Je kunt ze dan altijd weer terug vinden.
**Eigenlijk ook de controle of het de persoon is die aangegeven staat op het aanvraagformulier?**Ja. Ik heb vanmorgen vier mensen aan de balie gehad met dezelfde achternaam. En als ik daar achteraf op terug ga zoeken dan heb ik nooit meer iets om dat te controleren. Daarom wil ik het BSN nummer hebben want dat is echt persoonsgebonden.
**En wordt dat dan ook uitgelegd waarom dat gevraagd wordt?**
Als mensen daarom vragen, ja.
**Vragen mensen daar wel eens om?**
Een heel enkel keertje. Je hebt wel eens mensen die dan zeggen, ik ben hier toch niet voor het eerst. En dan probeer je dat uit te leggen maar dan luisteren ze eigenlijk al niet meer.
**Dan zijn ze het er niet mee eens.**
Nee.
**Krijgen cliënten nog meer informatie van jullie over hoe bijvoorbeeld hun gegevens worden opgeslagen ect?**
Nee, eigenlijk nooit. Moet ik heel eerlijk zeggen. Als er mensen zijn die daar vragen over zouden hebben dan krijgen ze daar natuurlijk uitleg over. Maar er is ook bijna nooit iemand die daar naar vraagt, hoe dat zit.
**En hebben jullie wel folders eventueel om te geven als ze er naar vragen?**
Nee. We hebben daar geen folders voor.
**Wordt aan de cliënt uitgelegd hoe de uitslag gedeeld wordt met bijvoorbeeld de huisarts?**
We melden dat de uitslag naar de huisarts gaat, of de aanvragend arts moet ik zeggen. En als mensen het perse zelf willen hebben, dan mag dat. Maar dan moeten ze het zelf komen ophalen en zich legitimeren.
**Maar dan moeten ze er zelf mee komen, met die vraag?**
ja.
Zijn er bepaalde informatiebronnen als het gaat om privacy die je gebruikt?
Nee. En als we dingen niet weten dan kunnen we in het VECOZO programma kijken, hoe het zit met de verzekering. Dat kunnen we wel.
Dat is dan met het zorgverzekeringspasje dat je iemand kan opzoeken?
Of met het BSN nummer. Maar dat is meer voor de mensen die niet verzekerd zijn. Ze komen wel eens met een pasje die verlopen is.
Maar dat doen jullie dus niet standaard. Alleen als jullie twijfels hebben of iemand verzekerd is of niet?
Precies.
Hebben jullie hier ook andere bronnen zoals handleidingen of iets dergelijks?
Niet dat ik weet.
Ik begreep ook dat er Sopdocumenten zijn die gebruikt kunnen worden. Gebruiken jullie die ook?
Nee, eigenlijk niet.
Is daar een reden voor?
We hebben hier bij de receptie het zelf helpen maken, dus we weten het eigenlijk wel. Wel als we nieuwe collega’s krijgen dan verwijzen we daar naar. En wat ze daar vervolgens mee doen..
Maar jullie weten het wel te vinden in elk geval?
Ja, volgens mij wel. We hebben het volgens mij zelfs hier liggen.
**Alle gegevens die jullie tijdens jullie werkzaamheden voorbij zien komen, hebben jullie hier een geheimhoudingsplicht voor?**
Ja.
**Dat is ook wel duidelijk voor iedereen?**
Ja.
**En alle gegevens die ingevoerd worden, hoelang blijven die bewaard?**
Bloeduitslagen kan ik denk ik heel lang terug kijken. Soms wel een jaar of tien terug.
Soms is het wel eens handig als de patiënten zelf er nog om vragen. Die kunnen ze dan krijgen.
**Gebeurt dat vaak, dat patiënten het zelf op komen vragen?**
Steeds vaker. Patiënten worden natuurlijk steeds mondiger en dat kan je in dat opzicht ook merken. Ze zeggen dan, dat zijn mijn uitslagen en ik wil weten hoe of wat. En dan zeggen wij wel dat zij de uitslag krijgen van ons maar als ze daar uitleg over willen dan moeten ze toch naar de huisarts.
**Mocht er per ongeluk gegevens op straat belanden, dat de gegevens aan de verkeerde persoon worden verstrekt ect. Is het dan voor jullie duidelijk wat jullie moeten doen? Is daar een protocol voor?**
Dat weet ik niet. Maar verkeerde patiënten aan elkaar gekoppeld dat gaat naar achter.
**Naar medical services, toch?**
Ja. En uitslagen aan de verkeerde personen dat gebeurd niet want ik vraag altijd aan de balie of ze willen kijken of het hun uitslagen zijn.
**Er staat op het aanvraagformulier een hokje dat aangevinkt kan worden als de cliënt bezwaar heeft tegen gebruik van lichaamsmateriaal voor wetenschappelijk onderzoek. Bespreken jullie dit met de cliënt?**
Soms wel. Als de cliënt het formulier nog moet invullen dan stellen ze daar wel eens een vraag over. Dan leggen we het inderdaad uit dat als we de apparatuur willen testen dat we daar dan ‘oud’ bloed voor gebruiken. Er zijn eigenlijk maar weinig mensen die daar dan bezwaar tegen hebben. Soms wel en dan kruisen ze het aan.
**En dat is dan het enige waarvoor het bloed gebruikt zal worden?**
Voor zover ik weet wel.
**En op het moment dat ze al met een ingevuld formulier komen dan vragen jullie daar niet specifiek naar?**
Nee.
**Zijn er ook nog andere zaken die besproken worden met de cliënt?**
Voor de rest niet.
**Wat betreft de andere handelingen die jullie uitvoeren. Ik weet niet of jullie ook uitslagen doorgeven?**
Ja.
**Nemen jullie dan nog extra maatregelen? Als er bijvoorbeeld gebeld wordt voor een uitslag?**
We geven geen uitslagen door aan de telefoon, ook niet aan artsen of patiënten. Als artsen perse willen dat er een uitslag wordt doorgegeven aan de telefoon dan verbinden we ze door met de klinisch chemicus of microbioloog. En als patiënten de uitslagen willen hebben, die krijgen ze in ieder geval niet. Of ze moeten naar de arts of hier langs komen en zich legitimeren.
**In feite als iemand jullie belt is het enige dat jullie doen ze telefonisch doorverbinden of aangeven dat uitslagen niet telefonisch worden doorgegeven.**
Zoals nu, we hebben dan sleutelnet (zorgdomein) en we hebben dan een artsencode dus dan weet je dat het een arts is. En daarna wordt het dan in sleutelnet gezet.
**Dus dan kun je het controleren?**
Ja.
Als zij dan een ‘sleutelnetcode’ aan jullie geven..
Ja, en dat is hetzelfde met faxen. Dan kan het niet mis gaan.
**En als je toch twijfelt over de code van sleutelnet of van de fax?**
Dan gaan we overleggen. We hebben het één keer gehad met een dame die had er zelf een faxnummer bij gezet. En wij twijfelde een beetje want bij de arts die erop stond, daar stond al een faxnummer bij. Toen zijn we dus gaan kijken of we het faxnummer ergens konden terugvinden. Dat lukte niet. Toen hebben we het uiteindelijk ook niet gefaxt.
**Dus jullie checken het wel altijd. En als jullie het niet vertrouwen dan gaan jullie overleggen?**
Inderdaad. Als we twijfelen gaan we altijd naar de klinisch chemicus om te vragen wat we er het beste mee kunnen doen.
**Het komt er dus op neer dat jullie uitslagen delen via de fax, sleutelnet (zorgdomein) en met uitzondering telefonisch via de klinisch chemicus?**
Dat klopt.
**Zijn er verder nog zaken waar jullie rekening mee houden als het gaat om privacy binnen jullie werkzaamheden?**
Als er mensen zijn aan de balie voor een onderzoek waar wij meer informatie voor moeten hebben (zoals een soa test) dan nemen we de mensen altijd even mee naar een aparte ruimte. Dan kunnen we het overleggen zonder dat de hele wereld het hoor, waar je het over hebt.
Het gebeurd ook wel een enkele keer dat de uitslag niet naar de huisarts of verzekering mag.
**Dan komen ze de uitslag zelf ophalen?**
Klopt. Dan moeten we het wel even in de gaten houden dat die uitslag niet naar een arts of andere aanvrager toe wordt gezonden.
**Geeft de cliënt dat dan zelf aan?**
Meestal begint de cliënt daar zelf al over.
**(Telefoontje komt binnen) En dit is dan iemand die belde over een uitslag?**
Een assistente die belde dat een uitslag nog niet was binnengekomen via sleutelnet.
**En dan vraag je altijd de geboortedatum en achternaam?**
Ja. Anders weet ik niet welke patiënt het is.
**Ik heb al mijn vragen wel gesteld. Heb jij misschien nog vragen of opmerkingen voor mij?**
Ja. We hebben nog een maatregel dat formulieren die van patiënten weg moeten worden in een speciale bak, die bij onze balie staat met sloten erop, gedaan.
**Formulieren die vernietigd moeten worden?**
Ja.
**En dat gaat dan naar een speciaal vernietigingsbedrijf?**
Ja, het gaat in een nog grotere bak dan die wij hebben staan en dat wordt dan vernietigd.
**En wat voor een formulieren zijn dat dan?**
Aanvraagformulieren die bijvoorbeeld dubbel zijn verzonden, formulieren die wij hebben ontvangen maar de mensen komen niet ect.
**Want de aanvraagformulieren die ingediend worden moeten bewaard blijven maar als het bijvoorbeeld dubbel is dan mag het vernietigd worden?**
Ja.
**Zijn er zelf nog zaken waarvan je zegt dat mis ik nog over privacy of daar zou meer duidelijkheid over moeten komen?**
Het zou in ieder geval niet verkeerd zijn om foldermateriaal te hebben met informatie over wat er met de gegevens van patiënten gebeurd en waarom bijvoorbeeld het BSN nummer moet worden gecontroleerd. Dan kan je daar altijd naar verwijzen.
**Ik denk dat ik wel voldoende weet. Dankjewel.**

SCAN medewerker: Carolien

|  |  |  |
| --- | --- | --- |
|  | Ja/Nee | Toelichting |
| 1. Wordt de cliënt gewezen op zijn rechten(recht om vergeten te worden, inzagerecht ect.) met betrekking tot privacy bij zijn/haar contact met de betreffende medewerker?  | Nee |  |
| 2. Wordt aan de cliënt uitgelegd om welke reden de persoonsgegevens (zoals BSN nummer) dienen te worden verwerkt? | Nee | Mits zij er naar vragen dan krijgt de cliënt een uitleg |
| 3. Wordt er toestemming gevraagd voor verwerking van persoonsgegevens aan de cliënt? | Nee |  |
| 4. Indien ja, wordt deze toestemming schriftelijk vastgelegd? | - |  |
| 7. Wordt aan de cliënt uitgelegd op welke wijze zijn/haar persoonsgegevens gedeeld worden met de opdrachtgever (bijv. huisarts)?  | Nee | De cliënt mag wel vragen om de uitslag alleen met hem te delen en niet naar derden te versturen. Hier wordt de cliënt niet actief op gewezen |
| 8. Wordt aan de cliënt gevraagd of hij/zij bezwaar heeft tegen ander gebruik lichaamsmateriaal? | Nee | Cliënt dient het zelf aan te geven of daar vragen over te stellen |
| 9. Welke bronnen gebruikt u voor het uitvoeren van handelingen die bij het doen van onderzoek horen? | n.v.t. | Overleg met leidinggevende(n) |
| 10. Zijn er nog andere manieren om aan informatie te komen als er vragen zijn over privacy beleid? (checklisten, protocollen ect.)  | ja | De digitale bronnen (Sops via Wiki) , die we ook hardcopy in de kast hebben staan |
| 11. Als het gaat om bedrijfsgegevens heeft u dan een geheimhoudingsplicht?  | Ja |  |
| 12. Weet u hoe lang persoonsgegevens dienen te worden bewaard?  | Nee | Ik kan wel bloeduitslagen van zeker 10 jaar geleden terug vinden |
| 13. Bent u op de hoogte van de maatregelen die getroffen dienen te worden als er sprake is van een datalek? | Nee |  |
| 14. Bent u zich bewust van de wet- en regelgeving op het gebied van de privacy van cliënten?  | Ja |  |

**Datum: 10-08-2016
Afdeling: Laboratorium
Medewerker: Joyce Zwarts
Functie: Basis analist
In dienst sinds: augustus 2009

Ik zal eerst even uitleggen ik hier precies aan het doen ben. Ik zit hier voor mijn afstuderen en doe onderzoek naar het privacy beleid binnen SCAL en dan richt ik mij op het bloedonderzoek. Dus eigenlijk vanaf het moment dat iemand hier binnenkomt met een aanvraagformulier tot aan de verwerking van de uitslag. En in die weg bekijk ik hoe er om gegaan wordt met de privacy van de cliënten die hier komen.
Kun je mij in z’n algemeenheid vertellen welke handelingen je zoal doet als het gaat om bloedonderzoek?**Wat ik doe is, ik ontvang in principe de monsters. We krijgen materialen van de spreekuren hier maar ook van de spreekuren buiten en de huisvisites doormiddel van de bodes of de mensen die de huisbezoeken doen. En dan beginnen we met het materiaal in de centrifuge te zetten, dat wordt afgedraaid. Inmiddels worden dan de formulieren, als dat niet papierloos is want daar zijn we net naar over en dat is ook een beetje zoeken, dat wordt ingevoerd en als het in Laboses gearriveerd is dan kunnen we het gaan verwerken. Dan gaat het de sorteerrobot in en die gaan al de buisjes neer zetten waar ze horen, zeg maar. En dan vanaf dat moment gaan ze het apparaat in. Verder houden we de sorteerboom bij en de bepalingen die wij niet zelf kunnen doen sturen wij door naar externe laboratoria. Dus daar draaien we lijsten voor uit en die moeten we verwerken. Dat wordt dan neergezet zodat de bodes die kunnen ophalen. En ook wordt het per post naar andere laboratoria gestuurd. En we voeren uitslagen in die terugkomen van externe laboratoria.
**Wordt er bij de uitvoering van al die handelingen rekening gehouden met de privacy?**
We werken dan natuurlijk vooral met labnummers en zien daar niet echt de patiënt achter. Wel op de verzendlijsten, daar staan wel naam en geboortedatum op maar dat is echt puur om te checken heb ik de goede buis van de goede patiënt met de goede aanvraag. Voordat het naar het externe laboratorium toe gaat.
En op het moment dat bloed onderzocht wordt dan zetten jullie dat allemaal klaar en dan gaat het waarschijnlijk naar de analist en die zal het dan verder verwerken?
Klopt. Die zet het weer in het apparaat en de cijfers gaan dan weer automatisch naar Laboses.
**Dat gaat allemaal automatisch?**
Ja.
**Jullie hebben weinig patiëntengegevens in handen?**
Ja, hooguit naam en geboortedatum maar dat is negen van de tien keer als we afwijkende uitslagen hebben. Die dan naar de huisarts doorgebeld dienen te worden. Dan kom je er wel mee in aanraking want je moet wel weten om welke patiënt het gaat. Maar over het algemeen werken wij heel veel met nummers. Voor ons is het vaak van, ik ben op zoek naar dit nummer.
**En niet op naam?**
Nee want alles staat op nummer.
**Controleer je dan nog wel het aanvraagformulier?**
Nee, in principe wordt het ingevoerd en dan worden de gegevens erbij opgezocht om te controleren of het de goede patiënt is. En dan wordt het nummer gekoppeld aan het nummer van de patiënt.
**Bellen jullie ook uitslagen door?**
Ja.
**Neem je dan maatregelen om de privacy te waarborgen?**
In principe faxen we de uitslagen eerst naar de huisarts. Op het moment dat je belt dan check je natuurlijk wel of je de juiste praktijk aan de telefoon hebt.
**Hoe check je dat?**
Meestal hoor je het gelijk want dan zeggen ze meteen van welke praktijk ze zijn. Maar soms als je naar een buitenlijn belt willen ze nog wel eens opnemen met alleen de voornaam. Dan check je wel van bel ik met deze huisartsenpraktijk. En dan vragen we eigenlijk in eerste instantie hebben jullie de fax gehad. En dan gaan ze eerst daar naar kijken en dan hoor ik vaak van hun al om welke patiënt het gaat en dat kan ik dan bevestigen. Daar heb je dan ook al een check in, zeg maar. Voordat je alles deelt.
**Toestemming van de cliënt, daar hebben jullie eigenlijk niks mee te maken?**
Nee.
**Stel je bent aan het werk en je hebt vragen over privacy of weet je niet hoe je het beste met iets om moet gaan. Misschien heb je iemand aan de telefoon waarvan je niet zo goed weet wat je er mee moet. Wat doe je dan?**
Ik overleg meestal dan met mijn collega’s.
Maar dat gebeurd eigenlijk niet.
**Omdat het al duidelijk voor jou is, welke kaders en richtlijnen?**
Ja, precies. En ik heb zelf ook heel lang bij medical services gezeten en daar heb je met van alles te maken. Patiënten, ziekenhuizen, artsen ect dus ik ben dat wel gewend. Nu heb ik maar een heel klein gedeelte, alleen de aanvragend arts vaak. Die belt over welk onderzoek hij moet aankruisen voor wat hij onderzocht wil hebben en dan komen vaak de patiëntgegevens niet aan bod. Dus dat zijn eigenlijk de enige contacten die wij hebben met externen die wij hebben.
Natuurlijk hebben wij wel, dat als wij iets naar Antwerpen hebben verstuurd, de huisarts belt van kunnen jullie nog iets er bij aanvragen. Maar dan werken we weer met het aanvraagnummer want die kunnen wij dan weer opzoeken in het systeem. Zij checken dan wel weer van klopt het in ons systeem. Wij werken veel met nummers.
**Dat best handig, denk ik.**
Ja. Het is lastig om met achternamen te werken.
**Gebruik je ook nog andere informatiebronnen zoals internet, handboek ect ?**
Ik gebruik wel eens internet als ik een uitslag van een arts niet helemaal begrijp om te achterhalen wat hij daar nou mee bedoelt.
**Maar over privacy of regels daarover niet?**
Nee, eigenlijk niet.
Ik vind het ook soms wel heel ver gaan. Kijk, privacy daar ben ik best een groot voorstander. Maar op het moment dat je als zorgverlener niet eens meer met elkaar dingen mag uitwisselen, dat gaat soms best ver. We hebben ook wel te maken met een oudere generatie, met de vergrijzing ect Die zijn niet altijd even bijdehand en begrijpen niet altijd wat er bedoelt wordt. En dan moet je aan zo’n iemand vragen of ze toestemming wil geven om gegevens met hun specialist te mogen uitwisselen. Dat snappen ze niet. Dan denk ik wel eens hoe ver gaan we.
**Doen jullie dat wel, toestemming vragen voor het uitwisselen van gegevens met specialisten?**Wij zelf niet. Maar we hebben natuurlijk wel bij Medical services dat er ziekenhuizen bellen voor de bloeduitslagen en dat we dan moeten zeggen dat we het niet zomaar mogen geven omdat de huisarts de aanvrager is. Dat vind ik zo krom.
**En ze werken gewoon samen, natuurlijk.**
Ja. En dat vind ik dan wel heel ver gaan. Je kunt ook doorschieten met de privacy gevoeligheid. **Dat gaat dan ten koste van de zorg?**
Ja, en ik vind al dat het allemaal een hoop geld kost en dat je er bijna niks meer van terug ziet. En als de samenwerking dan ook al niet meer mag dan mag je wel extra mensen in gaan huren. Wie gaat dat dan weer betalen. Ik vind het heel ver gaan.
Kijk, dat je in een wachtruimte niet heel hard alle gegevens roept dat moet je niet willen. Maar als je gegevens niet meer mag doorsturen naar een specialist waar die patiënt ook in behandeling is dan is dat wel een probleem. Die specialist belt niet voor niks. Dus ik vind dat ver gaan, heel ver gaan.
**Heb je ook geheimhoudingsplicht?**
Ja. Ik mag niet over patiënten praten thuis. Dat is logisch als je in de zorg werkt.
Je ziet natuurlijk toch wel dingen soms dat je denkt van, die ken ik. En zeker met zwangere mensen dan weet je het vaak eerder dan dat de familie het van die persoon weet. En dan weet je dat je gewoon je mond moet houden, klaar. Ik bedoel dat hoort bij je vak.
**Alle gegevens die je invoert, weet je ook hoe lang dat bewaard blijft?**
Ja, volgens mij heel lang. Als er een externe laboratoria is dan hoeven wij het zelf maar drie maanden te bewaren. En voor ons dacht ik vijftien jaar.
**En stel dat er bijvoorbeeld een buis vermist is, of het aanvraagformulier kwijt is. Het kan natuurlijk ook voorkomen dat je per ongeluk gegevens met iemand heb gedeeld die dat niet zou moeten weten of dat er toch iets kwijt raakt. Weet je dan ook wat je moet doen?**
Ik gok een melding schrijven. Dat moeten we altijd als we fouten maken.
**En hoe gaat dat dan?**
We hebben daar speciale meldingsformulieren voor. Die vul je dan helemaal in, om welke patiënt het gaat en wat er gebeurd is, welke stappen je ondernomen hebt en wat de suggesties zijn om de fout te voorkomen voor de volgende keer. En die gaat dan naar de kwaliteitsfunctionaris en die gaat daarmee aan de slag.
**Die neemt het verder in behandeling?**
Ja.
Ik moet zeggen dat ik nog nooit gegevens heb gedeeld met iemand waar het niet thuis hoort. Je weet allemaal dat als je een voicemail krijgt dat je niet in spreekt.
**Ben je je bewust van de wet- en regelgeving als het gaat om privacy?**
Een stukje wel. Van wat voor mij van toepassing is. Er zullen ongetwijfeld dingen in staan waarvan je denkt, dat is voordelig en dingen waarvan ik al zei ik vind het soms ook ver gaan.
Je wilt de snelste en beste zorg aan iemand geven en als je dan eerst moet vragen of iemand toestemming wil geven dan kan je inmiddels al begraven zijn. Daar heb ik echt moeite mee.
Waar is de grens. En ik denk je wilt als zorgverleners het beste voor de patiënt dus waarom mag je dat dan niet delen met elkaar, denk ik dan. En zeker bij de oudere generatie, die meer moeite heeft met toestemming geven omdat ze het allemaal niet zo snappen, dan is het lastig.
**Heb je nog vragen aan mij?**
Nee. En wat wij aan privacy kunnen doen daar zorgen we gewoon voor. Alles wordt op een nette manier verwerkt.

SCAN medewerker: Joyce Zwarts

|  |  |  |
| --- | --- | --- |
|  | Ja/Nee | Toelichting |
| 1. Wordt de cliënt gewezen op zijn rechten(recht om vergeten te worden, inzagerecht ect.) met betrekking tot privacy bij zijn/haar contact met de betreffende medewerker?  | n.v.t. |  |
| 2. Wordt aan de cliënt uitgelegd om welke reden de persoonsgegevens (zoals BSN nummer) dienen te worden verwerkt? | n.v.t. |  |
| 3. Wordt er toestemming gevraagd voor verwerking van persoonsgegevens aan de cliënt? | n.v.t. |  |
| 4. Indien ja, wordt deze toestemming schriftelijk vastgelegd? | - |  |
| 7. Wordt aan de cliënt uitgelegd op welke wijze zijn/haar persoonsgegevens gedeeld worden met de opdrachtgever (bijv. huisarts)?  | n.v.t. |  |
| 8. Wordt aan de cliënt gevraagd of hij/zij bezwaar heeft tegen ander gebruik lichaamsmateriaal? | n.v.t. |  |
| 9. Welke bronnen gebruikt u voor het uitvoeren van handelingen die bij het doen van onderzoek horen? | n.v.t. | Wiki (Sopdocumenten) en de leidinggevende(n) |
| 10. Zijn er nog andere manieren om aan informatie te komen als er vragen zijn over privacy beleid? (checklisten, protocollen ect.)  | Nee | Alleen de digitale bronnen en leidinggevende(n) |
| 11. Als het gaat om bedrijfsgegevens heeft u dan een geheimhoudingsplicht?  | Ja |  |
| 12. Weet u hoe lang persoonsgegevens dienen te worden bewaard?  | Ja | Ik dacht 15 jaar en voor externe uitslagen geldt 3 maanden |
| 13. Bent u op de hoogte van de maatregelen die getroffen dienen te worden als er sprake is van een datalek? | Ja | Meldingsformulier invullen, die gaat naar de kwaliteitsfunctionaris |
| 14. Bent u zich bewust van de wet- en regelgeving op het gebied van de privacy van cliënten?  | Ja | Alleen de zaken die relevant zijn voor mijn werkzaamheden |

**Datum: 10-08-2016
Afdeling: Laboratorium
Medewerker: Esther Geerlings
Functie: Analist
In dienst sinds: 2004

Ik heb net ook al Joyce gesproken, zij is basisanalist. Zij vertelde wat haar werkzaamheden zijn en daarna komt het bij jullie terecht.**Zij verzorgt met name de verzending en ik zorg eigenlijk voor de getallen bij de cliënten.
**Dat is dan daadwerkelijk het onderzoek?**
Ja.
**Ik richt mij voornamelijk op het bloedonderzoek en volg dan de weg die de cliënt volgt. Vanaf het moment dat zij zich melden bij de receptie met het aanvraagformulier tot aan het moment dat de uitslagen worden verwerkt en gearchiveerd.
Ik vroeg mij af waar jullie rekening mee houden tijdens jullie handelingen op het gebied van privacy? Hebben jullie al hele duidelijke maatregelen?**
Het wordt in ieder geval gevraagd aan de patiënt. Voor de rest eigenlijk niet zoveel denk ik. De monsters zijn bij ons een nummer en wie daarachter zit daar denken wij niet zo over na. En dat nummer kun je natuurlijk wel koppelen in de computer aan de uitslag. Maar over het algemeen van de honderd buizen kijk je bij eentje misschien van goh, is het een heel oud iemand ofzo..
**En dat is eigenlijk meer als het onderzoek afwijkend is en je meer informatie nodig hebt?**
Ja.
**En als het niet opvallend is en het is gewoon een ‘normaal’ onderzoek dan kijken jullie niet eens naar de persoonsgegevens?**
Nee, helemaal niet.
**Want het wordt automatisch door het apparaat in Laboses gezet?**
Ja. Het komt binnen via Laboses en wordt ook weer gerapporteerd via Laboses.
**Dus op het moment dat er echt niks afwijkends is dan hebben jullie geen persoonsgegevens in handen?**
Nee, echt niet. Alleen maar nummers.
**En op het moment dat jullie dat wel hebben en jullie hebben contact met de huisarts of een andere aanvrager voor het onderzoek, wat wordt er dan besproken?**
Nou als er afwijkende uitslagen zijn dan faxen we de uitslagen eerst. We geven niet de getallen maar vragen of ze de fax hebben ontvangen, ja of nee.
**Wordt er dan ook alleen in nummers gepraat of wordt er dan wel een BSN nummer of iets dergelijks gedeeld?**
Nee, je zegt alleen de achternaam van de patiënt en eventueel de geboortedatum. Maar BSN nummer niet en vaak zegt de huisarts ook al van oh, die meneer heb ik gezien, dan weet ik het al. Wij vragen voornamelijk of ze de fax hebben ontvangen. Dan moeten we natuurlijk wel de achternaam zeggen anders weet je niet over wie het gaat.
**Op het moment dat iemand jullie belt, controleren jullie dan nog wie jullie aan de lijn hebben?**
Nee.
**Dus als iemand zegt van, ik ben de huisarts van die en die dan is dat voldoende?**
Dat zou kunnen. En soms heb je wel eens argwaan.
**Maar dan kan het wel zijn dat jullie dan vragen naar welk faxnummer zou het moeten?**
Ja. In principe geven wij geen uitslagen telefonisch door. Maar het gebeurd natuurlijk wel eens dat mensen slinks door een…. Of een heel aannemelijk verhaal hebben.
**Dan wordt het soms wel eens gedaan?**
Ja. Kijk bijvoorbeeld als er snel gereageerd moet worden en een arts belt om navraag te doen naar een bepaalde waarde, dan zeg ik niet van zal ik het even invoeren. En vaak heb je het dan wel al gefaxt. Maar dan is het soms wel even moeilijk, ja.
**Omdat die tijdsdruk er dan is?**
Ja.
**Dus dan ga je het niet eerst allemaal verifiëren maar dan geef je het gewoon door?**
Ja.

**Jullie hebben niet direct contact met de cliënt zelf?**
Nee, eigenlijk nooit.
**Wordt er bloed of ander lichaamsmateriaal gebruikt voor onderzoek anders dan waar om gevraagd is?**Ja. Voor validatie.
**Dat is om de apparaten te testen?**
Ja.
**Kijken jullie dan ook naar of het vinkje is aangekruist op het aanvraagformulier**…
Ja, er is één groep van patiënten van een instelling ergens en dan weten we zeker dat we dat zeker niet moeten gebruiken.
**Want er is ook een optie op het aanvraagformulier waarop staat aangegeven of cliënt bezwaar heeft tegen het gebruik van lichaamsmateriaal voor wetenschappelijk onderzoek. Controleren jullie dat altijd?**
Dat gebeurd niet altijd. We zijn ook met validatie bezig dus als jij hele hoge uitslagen wil. Maar dan anonimiseren we het wel.
**Dus dan is het niet meer te herleiden naar de cliënt?**
Nee. We nummeren het dan.
**Mocht er nou iets zijn waar vragen over zijn met betrekking tot privacy. Zoals twijfel bij het doorgeven van uitslagen ect zijn er dan bepaalde bronnen die je dan kan gebruiken?**
Ja, je kunt naar de klinisch chemicus gaan. We hebben ook wel eens dat er bijvoorbeeld een faxnummer genoteerd staat waarvan wij zoiets hebben van klopt dat wel. Dan is dat niet aan mij natuurlijk.
**Zijn er ook nog andere bronnen, zoals internet of handboeken ect die je kunt gebruiken voor als er vragen zijn?**
Ja, die zijn er wel.
**Gebruik je die ook?**
Je gebruikt het niet dagelijks. Maar als je daar op terug wilt vallen dan zijn ze er wel.
**Je weet ze wel te vinden?**
Ja.
**Als het gaat om alle gegevens die zoal voorbij komen. Jullie zien vooral nummers maar jullie zijn natuurlijk ook wel eens persoonsgegevens voorbij komen. Hebben jullie dan ook geheimhoudingsplicht?**
Ja.
**En alle gegevens worden ingevoerd, volgens mij steeds meer digitaal, weet u hoelang die bewaard worden?**
Het wordt gewoon digitaal verwerkt eigenlijk. En dan wordt het drie, vier keer per dag naar sleutelnet (zorgdomein) gestuurd. Hoelang het bewaard moet blijven staat ook in de Sops. Heel veel gaat natuurlijk digitaal dus dat weet ik niet precies. Voor de opslag op papier is het drie maanden geloof ik, en bloedgroepen bewaren we zelfs langer. Weet je, we hebben dozen beneden en dan per maand gaan we wisselen. En dan voor de ene bepaling staan er vier dozen dan weet je dat je die veel langer moet bewaren. En voor de andere staat één doos waar je om de drie maanden… dus het is een beetje wisselend. En bij sommigen staan er niet eens gegevens op dan zijn het alleen lijsten.
**Dan is het geanonimiseerd?**
Ja, eigenlijk wel.
**Stel er is een buis of aanvraagformulier vermist, of dat jullie een uitslag hebben doorgegeven aan de verkeerde persoon of dat er iets met de computer mis gaat. Dat noemen ze dan een datalek. Weten jullie dan ook, mocht zoiets gebeuren, wat er gedaan zou moeten worden? Is daar een procedure voor?**
Ik denk dat als er echt een datalek is, dat hebben wij niet zo snel door, dan zou ik naar IT gaan en eerst melden bij de klinisch chemicus. En dan gaan zij er verder mee aan de slag.
**Dus jullie weten wel waar het gemeld dient te worden en bij wie je terecht zou kunnen?**
Ja.
**Heb je zelf nog vragen over privacy. Of misschien is er iets waarvan je zegt daar moeten we meer over weten?**
We hebben een kast met dossier ook en ik denk, in het weekend zou daar in gekeken kunnen worden.

**Zijn dat dan patiëntendossiers?**
Ja. Één keer per maand worden die dossiers naar beneden gebracht, met uitslagen enzo.
**En die staan dan niet in een kast die op slot kan?**
Ze staan wel in een kast maar niet op slot.
**Alleen de deur is dan afgesloten?**
Er zit wel een slot op maar de laatste vrijdag die vergeet het nog wel eens.
**Dus daar zal misschien nog iets voor verzonnen moeten worden?**Ja. Op zich, het laboratorium is wel heel goed beveiligd. Ik werk dan wel eens op zaterdag en niemand kan eigenlijk voorbij één deur zonder een druppel.
**Dus niet iedereen kan zomaar het laboratorium in wandelen?**
Nee.

SCAN medewerker: Esther Geerlings

|  |  |  |
| --- | --- | --- |
|  | Ja/Nee | Toelichting |
| 1. Wordt de cliënt gewezen op zijn rechten(recht om vergeten te worden, inzagerecht ect.) met betrekking tot privacy bij zijn/haar contact met de betreffende medewerker?  | n.v.t. |  |
| 2. Wordt aan de cliënt uitgelegd om welke reden de persoonsgegevens (zoals BSN nummer) dienen te worden verwerkt? | n.v.t. |  |
| 3. Wordt er toestemming gevraagd voor verwerking van persoonsgegevens aan de cliënt? | n.v.t. |  |
| 4. Indien ja, wordt deze toestemming schriftelijk vastgelegd? | - |  |
| 7. Wordt aan de cliënt uitgelegd op welke wijze zijn/haar persoonsgegevens gedeeld worden met de opdrachtgever (bijv. huisarts)?  | n.v.t. |  |
| 8. Wordt aan de cliënt gevraagd of hij/zij bezwaar heeft tegen ander gebruik lichaamsmateriaal? | n.v.t. |  |
| 9. Welke bronnen gebruikt u voor het uitvoeren van handelingen die bij het doen van onderzoek horen? | n.v.t. | Wiki (Sopdocumenten) en de leidinggevende(n) |
| 10. Zijn er nog andere manieren om aan informatie te komen als er vragen zijn over privacy beleid? (checklisten, protocollen ect.)  | Nee | Alleen de digitale bronnen en leidinggevende(n) |
| 11. Als het gaat om bedrijfsgegevens heeft u dan een geheimhoudingsplicht?  | Ja |  |
| 12. Weet u hoe lang persoonsgegevens dienen te worden bewaard?  | Nee |  |
| 13. Bent u op de hoogte van de maatregelen die getroffen dienen te worden als er sprake is van een datalek? | Nee | Ik zou naar de klinisch chemicus en IT gaan |
| 14. Bent u zich bewust van de wet- en regelgeving op het gebied van de privacy van cliënten?  | Ja | Alleen de zaken die relevant zijn voor mijn werkzaamheden |

Bijlage 6.
 **Beroepsproduct in de vorm van een advies aan opdrachtgever SCAL**

De aanbevelingen kunnen geïnterpreteerd worden als een advies dat voortvloeit uit de bevindingen van het onderzoek. Het betreft een advies met het oog op de toekomstige algemene verordening gegevensbescherming dat vanaf het jaar 2018 volledig van kracht zal zijn. Met name omdat opdrachtgever SCAL nog tijd heeft aanpassingen in het beleid door te voeren lijkt het advies goed doorgevoerd te kunnen worden. Onderstaand de aanbevelingen.

**» Stel een functionaris privacy bescherming aan**
Mede omdat het privacy bewustzijn niet optimaal is en men privacy niet de belangrijkste prioriteit lijkt te geven is het verstandig een functionaris aan te stellen. Een persoon die privacy boven aan de lijst van de agenda plaatst en men kan wijzen op de consequenties als bepaalde zaken niet op tijd geregeld worden. Tevens zou de functionaris bepaalde onduidelijkheden over bijvoorbeeld het toestemmingsvereiste kunnen wegnemen door hier meer diepgang aan te geven middels een grondig onderzoek en overleg met bijvoorbeeld de instantie Autoriteit Persoonsgegevens.
**» Zorg voor een informatieplatform waar de cliënt naar kan worden verwezen als hij/zij een onderzoek komt laten uitvoeren.**
Het zal een toegankelijke manier van informatievoorziening moeten zijn. Denk aan folders, informatiescherm in de wachtruimte of meer informatie op de website. De onderwerpen die in ieder geval niet mogen ontbreken; welke rechten cliënten hebben, hoe lang en welke persoonsgegevens gearchiveerd worden, met wie en op welke wijze hun persoonsgegevens gedeeld worden, welke risico’s er bestaan bij verwerking van persoonsgegevens en op welke wijze deze ingeperkt worden en hoe het overig privacy beleid eruit ziet. In het bijzonder is aan te raden een uitleg te plaatsen over de legitimatieplicht alvorens een onderzoek. Hier komen regelmatig vragen over en die kunnen daarmee op eenvoudige wijze ondervangen worden. Alleen deze informatie delen op de website is niet voldoende, tijdens het cliëntencontact dient men op deze informatiebron gewezen te worden.
**»Zorg dat de toestemming van de cliënt voor de verwerking van zijn persoonsgegevens aan te tonen is op schriftelijke/digitale wijze.**
Er vanuit gaan dat de cliënt akkoord gaat met de verwerking van zijn persoonsgegevens, omdat dit bijvoorbeeld met de huisarts besproken is, is niet voldoende. Er dient aangetoond te kunnen worden dat de cliënt op de hoogte is van de wijze waarop zijn persoonsgegevens verwerkt worden en hiermee akkoord is gegaan. De verantwoordelijkheid ligt bij de organisatie waar de gegevens verwerkt worden, ongeacht welke verstandhouding er bestaat met cliënt. Op welke wijze de toestemming wordt vastgelegd is flexibel. Wel dient de toestemming mondeling of schriftelijk actief gevraagd te worden. Een optie zou kunnen zijn dat de vraag op het aanvraagformulier wordt aangevinkt bij een akkoord.
**»Zorg voor een risico analyse dat het privacy beleid van SCAL toetst en laat de resultaten hiervan vastleggen.**
Men dient een analyse te houden dat de risico’s binnen de organisatie wat betreft bescherming persoonsgegevens aan de oppervlakte legt. Vervolgens dient hierop geanticipeerd te worden en indien nodig (preventieve) maatregelen nemen. Het is belangrijk dat opdrachtgever SCAL kan aantonen dat deze analyse gehouden is en wat de eventuele vervolgstappen zullen zijn.
**»Zorg voor een protocol over de verwachte handelwijze bij constatering van een datalek en maak een register waar eventuele (kleine/grote) datalekken in genoteerd kunnen worden.** Prioriteit zou moeten liggen bij het voorkomen van datalekken. Indien er dan toch een datalek wordt geconstateerd moet iedere medewerker op de hoogte zijn hoe te handelen. Het beleid hierop dient te kunnen worden aangetoond.
**»Zorg dat alle medewerkers op de hoogte zijn van de (nieuwe) vereisten omtrent privacy beleid en hier ook naar handelt.**
De medewerkers hebben aangegeven privacy belangrijk te vinden en hier ook naar te handelen. Hier dienen zij wel duidelijke en toegankelijke handvaten voor te hebben. Zo is bijvoorbeeld het beleid rondom archiveren en vernietigen van documenten met persoonsgegevens vastgelegd. Het valt op dat de medewerkers ondanks de beschikbare documenten niet goed op de hoogte zijn van het beleid rondom het archief. De medewerkers die tijdens hun werkzaamheden in contact komen met cliënten dienen voorlichting te kunnen geven over het beleid rondom privacy. Hier moeten zij dan ook op correcte wijze over ingelicht zijn. Wellicht is het zaak om te achterhalen of de SOPdocumenten die momenteel beschikbaar zijn voor de medewerkers voldoet.
**»Leg eventueel contact met Autoriteit Persoonsgegevens voor advies rondom privacy beleid.**
De Autoriteit Persoonsgegevens (AP) heeft onder andere de taak voorlichting en advies te geven over bescherming van persoonsgegevens. Omdat er een complexiteit bestaat aangezien men met bijzondere (medische) persoonsgegevens te maken heeft zou het een mogelijkheid zijn om advies te vragen aan AP. Zij kunnen het privacy beleid beoordelen en toetsen aan de nieuwe wet- en regelgeving. Op deze manier heeft opdrachtgever SCAL alles gedaan om te voldoen aan de Algemene verordening gegevensbescherming.

1. ‘Zembla de jacht op uw medische gegevens’, NPO, 17 april 2014. [↑](#footnote-ref-1)
2. Richtlijn 95/46/EG
 [↑](#footnote-ref-2)
3. Art 4 lid 1 jo. Lid 2 sub j VWEU [↑](#footnote-ref-3)
4. Verdrag betreffende de werking van de Europese Unie, Rome, 25 maart 1957 [↑](#footnote-ref-4)
5. Art. 29 Europese Privacyrichtlijn 95/46/EG [↑](#footnote-ref-5)
6. Art. 1 Wbp [↑](#footnote-ref-6)
7. Art. 11 lid 2 Wbp [↑](#footnote-ref-7)
8. Art. 15 Wbp [↑](#footnote-ref-8)
9. MVT kamerstuk II 1998, 25892,3, hfst. 4.3 [↑](#footnote-ref-9)
10. MvT kamerstuk II 1998, 25892, 3, blz. 80 [↑](#footnote-ref-10)
11. Art. 5 lid 2 Wbp [↑](#footnote-ref-11)
12. Art. 7:455 BW [↑](#footnote-ref-12)
13. Art. 7:49 jo. 7:50 BW [↑](#footnote-ref-13)
14. Art. 51 lid 1 jo. Art. 52 Wbp [↑](#footnote-ref-14)
15. Kaderwet zelfstandige bestuursorganen, 2 november 2005 [↑](#footnote-ref-15)
16. Artikel 21 jo. 22 Kaderwet zelfstandige bestuursorganen [↑](#footnote-ref-16)
17. Art. 59A lid 1 Wbp [↑](#footnote-ref-17)
18. Art. 60 Wbp [↑](#footnote-ref-18)
19. Hoofdstuk 5 Handhaving, Algemene wet bestuursrecht, 01 januari 1994 en hoofdstuk 10 Sancties, Wet bescherming persoonsgegevens [↑](#footnote-ref-19)
20. Art. 66 Wbp [↑](#footnote-ref-20)
21. Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl>, Zoek op zoekwoorden; over privacy, wetten, wbp naslag, hoofdstuk 10, artikel 66 Wbp.  [↑](#footnote-ref-21)
22. Art. 75 Wbp [↑](#footnote-ref-22)
23. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 5 alinea 1 en bladzijde 6 alinea 2. [↑](#footnote-ref-23)
24. CBP Richtsnoeren: beveiliging van persoonsgegevens, BWBR0033572, 01 januari 2016 [↑](#footnote-ref-24)
25. Voorstel voor een verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, 2012/001, bladzijde 70 [↑](#footnote-ref-25)
26. Art. 1 sub d Wbp [↑](#footnote-ref-26)
27. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 41 alinea 1. [↑](#footnote-ref-27)
28. Autoriteit Persoonsgegevens, “De meldplicht datalekken in de wet bescherming persoonsgegevens”, 8 december 2015, bladzijde 7. [↑](#footnote-ref-28)
29. Kamerstukken II 2014/15, 33 662, nr. 11. [↑](#footnote-ref-29)
30. Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014. [↑](#footnote-ref-30)
31. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 40 alinea 2. [↑](#footnote-ref-31)
32. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 43 alinea 2. [↑](#footnote-ref-32)
33. Eerste kamer 2015/16, 33 169, AE, bladzijde 8. [↑](#footnote-ref-33)
34. Verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. [↑](#footnote-ref-34)
35. Art. 8 sub a Wbp [↑](#footnote-ref-35)
36. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 20 alinea 1. [↑](#footnote-ref-36)
37. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 19 alinea 3. [↑](#footnote-ref-37)
38. Artikel 12 lid 1 Verordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. [↑](#footnote-ref-38)
39. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 18. [↑](#footnote-ref-39)
40. HvJ (hoofdgeding en prejudiciële vragen) 13 mei 2014 C-131/12, Regel 20 onder 3. [↑](#footnote-ref-40)
41. HvJ 13 mei 2014 C‑131/12 [↑](#footnote-ref-41)
42. De gier-stam, ‘Waar gaat het heen met de Avg?’, nummer 6, augustus 2015 [↑](#footnote-ref-42)
43. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 28 alinea 2. [↑](#footnote-ref-43)
44. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 35 alinea 3. [↑](#footnote-ref-44)
45. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 39 alinea 2. [↑](#footnote-ref-45)
46. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 36 alinea 1. [↑](#footnote-ref-46)
47. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 39 alinea 1, bladzijde 45 alinea 4 en bladzijde 46 alinea 2. [↑](#footnote-ref-47)
48. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 53 alinea 2. [↑](#footnote-ref-48)
49. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 55 alinea 1 en 2. [↑](#footnote-ref-49)
50. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 67 alinea 2. [↑](#footnote-ref-50)
51. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 67 alinea 2. [↑](#footnote-ref-51)
52. Raad van de Europese Unie, Voorstel voor een verordening… … betreffende het vrije verkeer van die gegevens, 5455/16, 28 januari 2016, bladzijde 68 alinea 1. [↑](#footnote-ref-52)
53. Art. 51A Wbp [↑](#footnote-ref-53)
54. Art. 51a lid 1 Wbp [↑](#footnote-ref-54)
55. Art. 7 jo. 9 Wbp [↑](#footnote-ref-55)
56. Art. 453 WGBO [↑](#footnote-ref-56)
57. Art. 15 Wbp [↑](#footnote-ref-57)
58. Art. 3 WGBO
 [↑](#footnote-ref-58)
59. Kwaliteitshandboek Salux healthcare, versie 3, december 2015. [↑](#footnote-ref-59)
60. Privacy reglement Salux healthcare Leiden, versie 1.0, 01 oktober 2013. [↑](#footnote-ref-60)
61. Kwaliteitshandboek Salux healthcare, versie 3, december 2015. [↑](#footnote-ref-61)
62. Wiki, SOPMONST001, Aannemen van een aanvraag. [↑](#footnote-ref-62)
63. SCAL, [www.scal.nl](http://www.scal.nl) [↑](#footnote-ref-63)
64. Wiki, SOP DOCU011, Bewaartermijnen van documenten. [↑](#footnote-ref-64)
65. Wiki, KHBB6, Bewaartermijnen documenten. [↑](#footnote-ref-65)
66. Wiki, MONST001, aannemen van een aanvraag, 2015. [↑](#footnote-ref-66)
67. Wiki, RECP008, baliewerkzaamheden, 2011. [↑](#footnote-ref-67)
68. Wiki, RECP012, zoeken in VECOZO programma, 2014. [↑](#footnote-ref-68)
69. Wiki, RAPP001, rapportage, 2015. [↑](#footnote-ref-69)
70. Wiki, DOCU002, archiveren en vernietigen van documenten, 2014. [↑](#footnote-ref-70)
71. Wiki, LIJST007, te archiveren documenten, 2011. [↑](#footnote-ref-71)
72. Wiki, ADMI007, archivering aanvraagformulieren, 2011. [↑](#footnote-ref-72)
73. Wiki, KHBB6, bewaartermijnen documenten, 2014. [↑](#footnote-ref-73)
74. Wiki, MONST009, acties na overblijven van een buis, 2013. [↑](#footnote-ref-74)
75. Wiki, MONST008, acties na missen van een buis, 2011. [↑](#footnote-ref-75)