Gegevensbeschermingseffectbeoordeling (PIA)

PREZIES
surveillance van zorginfecties in ziekenhuizen en ZBC's

RIVM/CIb/EPI

(10)(2e) (10)(2e) t (10)(2e)

Bilthoven, 30 april 2020

RIVM/CIb/EPI - (10)(2e) (10)(2e) (10)(2e)

Vaststelling verwerkersverantwoordelijke: 30 april 2020
Naam: (10)(2e) (10)(2e)

Advies functionaris voor gegevensbescherming: 30 april 2020
Naam: (10)(2e) (10)(2e)

Advies CIO: 30 april 2020
Naam: n.v.t. binnen RIVM

Privacy officers (10)(2e) en (10)(2e)

Gegevensbeschermingseffectbeoordeling (PIA)

RIVM/CIb/EPI

(10)(2e) (10)(2e) (10)(2e)

Contact:

(10)(2e)
RIVM/CIb/EPI/ZIA
(10)(2e)@rivm.nl

Versie: 19 december 2019

Inhoudsopgave

Inleiding

Deze gegevensbeschermingseffectbeoordeling (PIA) is opgesteld ter beoordeling van de Surveillance van zorginfecties in ziekenhuizen en zelfstandige behandelcentra (zgn zorginstellingen voor acute zorg, verder in dit document zorginstellingen genoemd) onder de noemer van PREZIES; het surveillance systeem waarmee in de Nederlandse zorginstellingen zorginfecties worden geregistreerd.
Dit document bestaat uit drie onderdelen. Het eerste deel geeft een algemene beschrijving van de kenmerken van de gegevensverwerkingen. Het tweede deel bevat de beoordeling van de rechtmatigheid van de gegevensverwerkingen. In het derde deel wordt een beschrijving en beoordeling van de risico's voor betrokkenen gegeven. In het vierde deel worden maatregelen beschreven die de risico's kunnen mitigeren.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Deze PIA gaat over surveillance op gebied van infectieziekten, die wordt gecoördineerd door RIVM/CIb/EPI. Deze PIA betreft specifiek de surveillance van zorginfecties in ziekenhuizen en zelfstandige behandelcentra. Medische professionals werkzaam binnen deze zorginstellingen zijn gebonden aan het medisch beroepsgeheim.

Het PREZIES-netwerk (PREventie van ZIEkenhuisinfecties door Surveillance) is een samenwerkingsverband tussen zorginstellingen en het RIVM dat 3 typen van surveillance van zorginfecties (zgn. modules) uitvoert, te weten:

1. incidentiesurveillance van postoperatieve wondinfecties (POWI),
2. incidentiesurveillance van centraal veneuze katheter gerelateerde sepsis (lijnsepsis), en
3. puntprevalentiesurveillance (PPS) van alle typen zorginfecties.

De doelstellingen van het netwerk zijn het ontwikkelen, invoeren en onderhouden van een systeem van gestandaardiseerde surveillance, het genereren van vergelijkbare en landelijk representatieve gegevens, het doen en faciliteren van (interventie)onderzoek, en het faciliteren van interventies door samenwerking met andere partijen. Het uiteindelijke doel is het terugdringen van het aantal zorggerelateerde infecties in Nederland.

Binnen het netwerk worden door medische professionals in de deelnemende zorginstellingen gegevens verzameld over het optreden van zorggerelateerde infecties en over risicofactoren die de kans op het krijgen van een zorggerelateerde infectie beïnvloeden. Deze gegevens worden in de deelnemende zorginstellingen gepseudonimiseerd en per surveillancemodule opgenomen in de landelijke database voor infectieziekten OSIRIS op het RIVM.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Klik hier om infotekst te verbergen

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.
Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.
Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.
Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;

- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens
Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens
Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid
Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers
Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens
Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;

- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatieen locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.
In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
b. personen die voor een strafbaar feit zijn veroordeeld;
c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij **conceptregelgeving** kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

Binnen PREZIES worden van patiënten in zorginstellingen gegevens verzameld die betrekking hebben op het risico op, en het ontstaan/aanwezig zijn van, een zorginfectie. Zie ook de protocollen van de 3 modules op www.prezies.nl.

1. Patiënten:

Patiënten die in een Nederlandse zorginstelling (voor acute zorg, d.w.z. ziekenhuis, zelfstandig behandelcentrum (ZBC) of privékliniek) zijn opgenomen en/of zijn geopereerd. Hieronder vallen voor de modules POWI en PPS ook kinderen. Voor geen van de drie modules zijn er exclusiecriteria voor andere kwetsbare personen/groepen.

a) **Strafrechtelijke persoonsgegevens**: n.v.t. (worden niet verzameld).

b) **Gewone persoonsgegevens**:
Voor alle drie de modules hetzelfde:
geboortedatum, geslacht

c) Bijzondere persoonsgegevens:
Voor alle drie de modules hetzelfde:
Codes/nummers:
PREZIES ziekenhuis-code (nummer), versleuteld ziekenhuisspecifiek patiënt-identificatienummer, uniek databasenummer(OSIRIS-nummer), meldnummer dat ziekenhuizen in OSIRIS kunnen invullen.

Per module apart vermeld:
1. Postoperatieve wondinfecties (POWI) surveillance:
- Operatie- en opnamegegevens:
  type operatie (+ indien relevant of deze links of rechts plaatsvond), opnamedatum, operatiedatum, ontslagdatum.
- Risicofactoren voor infectie (POWI):
  lengte/gewicht/BMI, wondklasse, ASA-score, operatieduur, verdenking op maligniteit, plaatsing implantaat, vervolgoperatie + datum, diabetes, okselklierdissectie, directe reconstructie, aanleg stoma, naadlekkage, keizersnede primair/secundair.
- Infectiegegevens:
  aanwezigheid POWI, type POWI, infectiedatum, kweekresultaat, kweekdatum, gekweekte verwekker + resistentiepatroon van de verwekker.

2. Lijnsepsis surveillance
- Opname- en lijngegevens:
  opnamedatum, lijnnummer, soort lijn, inbrengdatum, einddatum surveillance.
- Risicofactoren voor infectie (lijnsepsis):
  specialisme, lokalisatie (vene), toepassing, IC opnamedatum, IC einddatum.
- Infectiegegevens:
  aanwezigheid lijnsepsis, soort lijnsepsis, infectiedatum, bacteriëmie bij inbreng, uitslagen bloed- en tipkweken: gekweekte verwekker + resistentiepatroon van verwekker.

3. Punt prevalentie surveillance (PPS)
- Opnamegegevens:
  opnamedatum.
- Risicofactoren voor zorginfectie:
  - Algemeen: registratiedatum, verpleegafdeling, specialisme hoofdbehandelaar + verpleegafdeling, infectie aanwezig op het moment van opname, IC opname, Soort IC, geboortegewicht (alleen voor baby's op IC), McCabe score.
  - operatie: operatie, operatiedatum, CTG hoofdgroep (wondklasse, vervolg OK).
  - hulpmiddelen: urethrakatheter + niveau aanduiding beoordeling urethrakathetergebruik, centraal veneuze katheter, perifere katheter, suprapubische katheter, arteriële katheter, invasieve beademing.
- Infectiegegevens:

aanwezigheid zorginfectie, soort zorginfectie, infectiedatum, kweekresultaat/gekweekte verwekker + resistentiepatroon van verwekker, ziekenhuisinfectie aanwezig bij opname, ontstaan in eigen instelling, type POWI, CTG hoofdgroep POWI, intravasale lijn-gerelateerd, focus secundaire sepsis, beademing gerelateerd (alleen bij pneumonie), urethrakatheter-gerelateerd (alleen bij urineweginfectie), gebruikte definitie zorginfectie.

- Antibioticagegevens:
  antibioticagebruik op dag van registratie,
  voor maximaal 3 elkaar direct opvolgende antimicrobiële middelen:
  soort antibiotica, toedieningsvorm, indicatie voor antibiotica + vermelding in dossier, type infectie, dosering chirurgische profylaxe, startdatum antibiotica, wijziging antibiotica, dosis antibiotica, startdatum vorige antibiotica met zelfde indicatie, niveau aanduiding beoordeling antibioticumgebruik

2. Artsen

De operateur die de ingreep in de POWI surveillance heeft uitgevoerd.

a) Strafrechtelijke persoonsgegevens: n.v.t..

b) Gewone persoonsgegevens:

De identiteit van de operateur kan optioneel d.m.v. een (in het ziekenhuis gepseudonimiseerde) 7-letterige code worden vastgelegd in de PREZIES POWI surveillance. Deze gegevens zijn voor PREZIES niet herleidbaar en worden door PREZIES ook niet gebruikt, maar registratie is mogelijk gemaakt om tegemoet te komen aan de behoeft van ziekenhuizen om de gegevens ook voor kwaliteitsverbetering (curatieve zorg) te kunnen gebruiken. De meeste ziekenhuizen maken hiervan geen gebruik. Zie voor meer informatie over dit gegeven onderdeel 4, 5 en 11 van deze PIA.

c) Bijzondere persoonsgegevens: n.v.t.

3. Contactpersonen (van ziekenhuizen/ZBC's/privéklinieken)

Voor alle drie de modules hetzelfde:

a) Strafrechtelijke persoonsgegevens: n.v.t..

b) Gewone persoonsgegevens:

contactgegevens (naam, e-mail, telefoonnummer, functie, werkadres), gebruikersnamen, gehashte wachtwoorden (gekoppeld aan organisatie, niet aan persoon),

c) Bijzondere persoonsgegevens: n.v.t.

4. Ouders van minderjarige betrokkenen

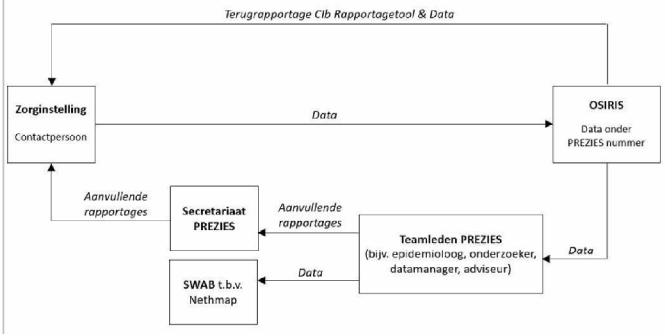
N.v.t.

3. Gegevensverwerkingen

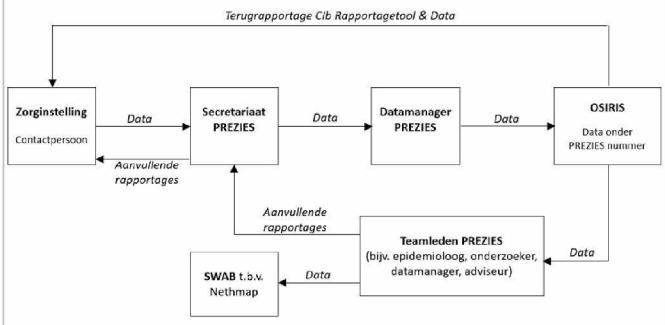
Geef alle voorgenomen gegevensverwerkingen weer.

In onderstaande flowcharts worden de gegevensverwerkingen van PREZIES gevisualiseerd.

Datastromen bij registratie rechtstreeks in OSIRIS:



Datastromen bij registratie in eigen databestand:



Het RIVM verwerkt hoofdzakelijk persoonsgegevens in het kader van de drie onderzoeksmodulen. Die vallen onder één doel: surveillance en wetenschappelijk onderzoek. Die gegevensverwerking wordt hieronder als eerst uitgewerkt. Daarnaast heeft het RIVM verwerkingen ingericht die niet noodzakelijk zijn voor surveillance en wetenschappelijk onderzoek, namelijk inzage en downloadmogelijkheid van de 'eigen' data

die organisaties invoeren, en de mogelijkheid om operateurnummer in te voeren in POWI-module. Die verwerkingen komen daarna aan bod.

Verwerking 1: Binnen het netwerk worden door de deelnemende zorginstellingen gegevens verzameld over het optreden van zorggerelateerde infecties en over risicofactoren die de kans op het krijgen van een zorggerelateerde infectie beïnvloeden. Deze gegevens worden in de deelnemende zorginstellingen gepseudonimiseerd en per surveillancemodule opgenomen in de landelijke database voor infectieziekten OSIRIS op het RIVM. Data worden ofwel rechtstreeks ingevoerd in OSIRIS, óf er wordt een compleet databestand via een beveiligde email verzonden naar (10)(2e)@rivm.nl, en via het secretariaat en de datamanagers opgenomen in OSIRIS. Het secretariaat fungeert hierbij als 'centrale ontvangst' terwijl de datamanagers zorgen voor een correcte invoer in OSIRIS, en controles uitvoeren op juistheid van de data. Waar nodig geven zij de zorginstellingen terugkoppeling ter correctie van de data. Zorginstellingen mogen zelf kiezen welke van de twee methodes voor aanleveren van de data zij willen gebruiken, de voorkeur verschilt per zorginstelling. De gegevens worden na elke inzending verwerkt en zijn per zorginstelling te downloaden uit OSIRIS (iedere zorginstelling kan alleen de 'eigen' gegevens downloaden). Ook is er door de zorginstellingen via een internetapplicatie (CIb rapportageomgeving) een terugrapportage op te vragen van de eigen gegevens, afgezet tegen op landelijk niveau geaggregeerde spiegelgegevens.
Per surveillancemodule worden de verzamelde gegevens door de medewerkers van PREZIES onder andere verwerkt in aanvullende rapportages, jaarlijkse (geaggregeerde) referentiecijfers, analyses t.b.v. wetenschappelijke artikelen, en verbetering van de surveillance. Rapportages worden via het secretariaat naar de deelnemers verzonden, de jaarlijkse (geaggregeerde) referentiecijfers worden gepubliceerd op de website van PREZIES. Hierin worden de afzonderlijke deelnemende zorginstellingen wel vermeld, maar worden de infectiecijfers van afzonderlijke zorginstellingen niet herleidbaar gepubliceerd. Eenmaal per jaar worden ongeaggregeerde gegevens over antibioticagebruik aan de SWAB verschaft ten behoeve van de NETHMAP rapportage.

Verwerking 2: PREZIES voorziet via Osiris in de mogelijkheid om een gepseudonimiseerde code voor de operateur in te voeren bij de POWI-module. Die mogelijkheid beantwoordt een behoefte uit sommige deelnemende organisaties. Niet alle deelnemende organisaties hebben die behoefte en niet alle organisaties maken gebruik van de mogelijkheid. De verwerkingen zijn niet noodzakelijk voor het onderzoek en hebben daarom een aparte grondslag nodig (zie 11.).

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.
Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van

personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt gedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.
Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

Doel van de PREZIES Surveillances is om inzicht en trends in zorginfecties en risicofactoren in kaart brengen om te adviseren over beleid t.a.v. preventie op gebied van zorginfecties in ziekenhuizen en ZBC's. Daarnaast kunnen de zorginstellingen hun eigen data (waar mogelijk gespiegeld aan geaggregeerde landelijke data) gebruiken voor aanvullende analyses en kwaliteitsverbetering op instellingsniveau.

1. Betrokkenen:

Gewone persoonsgegevens:
Nodig om patiënten in database uniek van elkaar te kunnen onderscheiden (zonder identificatie).

Geboortedatum daarnaast ook nodig om leeftijd te berekenen.

Bijzondere persoonsgegevens:

1. POWI surveillance:

- Operatie en opnamegegevens:
  nodig om de operaties te kunnen categoriseren v.w.b. type en operatiejaar, ontdubbelen van gegevens die dubbel in OSIRIS terecht zijn gekomen, berekenen van opnameduren en duur van operatie tot infectie etc.
- Risicofactoren:
  nodig voor risico-inschatting, trends in risicofactoren, berekening van additionele risico's, correctie voor verschil in patiëntenpopulaties (case-mix) tussen zorginstellingen, etc.
- Infectiegegevens:
  nodig voor berekenen infectiepercentages, duur van operatie tot infectie/kweek, evalueren van betrokken verwekkers (risico-inschatting), etc.

2. Lijnsepsis surveillance:

- Opname- en lijngegevens:
  nodig om aantal en type lijnen per patiënt te identificeren, de lijnduur te berekenen (nodig voor berekenen incidentiedichtheden), te ontdubbelen, etc.
- Risicofactoren:
  nodig voor risico-inschatting, trends in risicofactoren, berekening van additionele risico's, correctie voor case-mix, etc.
- Infectiegegevens:
  nodig voor berekenen infectiepercentages en incidentiedichtheden, aantal lijndagen tot infectie/kweek, evalueren van betrokken verwekkers (risico-inschatting), etc.

3. Punt prevalentie surveillance:

- Opnamegegevens:
  nodig om tijd tot infectie te berekenen, etc.
- Risicofactoren:
  nodig voor risico-inschatting, trends in risicofactoren, berekening van additionele risico's, correctie voor case-mix, etc.
- Infectiegegevens:
  nodig voor berekenen infectiepercentages, categoriseren soort zorginfecties, duur van opname tot infectie/kweek, evalueren van betrokken verwekkers (risico-inschatting), etc.
- Antibioticagegevens:
  nodig voor weergeven trends in antibioticagebruik, etc.

2. Artsen

Osiris biedt de mogelijkheid om een gepseudonimiseerde code voor de operateur in te voeren om deelnemende organisaties de mogelijkheid te bieden om ook operateurs in het overzicht van POWI-gevallen mee te nemen. Het invulveld is niet verplicht en wordt alleen gebruikt wanneer organisaties daar zelf belang bij ervaren.

3. Contactpersonen:

Gewone persoonsgegevens:

Nodig om contact op te nemen met uitvoerders van de surveillances.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke,

verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Verwerkersverantwoordelijke:
Voor beide verwerkingen is het RIVM verwerkingsverantwoordelijke. Het RIVM heeft het doel en de middelen bepaald voor de verwerkingen en handelt niet in opdracht van de deelnemende organisaties. Data zijn opgeslagen in de OSIRIS database die beheerd wordt door het RIVM. Alle teamleden van PREZIES en de bij de PREZIES surveillance betrokken medewerkers die nodig zijn om de landelijke surveillance in stand te houden/te verbeteren en analyses te doen op de data voor rapportages en wetenschappelijke publicaties (denk hierbij aan epidemiologen, onderzoekers, adviseurs, deskundigen infectiepreventie, RIVM-artsen, datamanagers en ICT-ers) hebben toegang tot de gepseudonimiseerde data. Rechten/authorisaties worden op directoryniveau geregeld.

Verwerker:
Relatics BV. Relatics is de leverancier van een online tool (administratie/beheer) die gebruikt wordt om de contactgegevens van deelnemende zorginstellingen en hun medewerkers op te slaan en te beheren. De voorwaarden waaronder gegevens in relatics worden beheerd zijn vastgelegd in de verwerkersovereenkomst die met Relatics BV is afgesloten. (zie bijlage)

Verstrekker:
De deelnemende ziekenhuizen, ZBC's en privéklinieken; zij nemen vrijwillig deel en leveren gepseudonimiseerde gegevens aan. Zij hebben tevens de sleutel van het gepseudonimiseerde patientidentificatienummer en gepseudonimiseerde code voor de operateur en zijn verwerkingsverantwoordelijk voor de verstrekking van persoonsgegevens.

Ontvanger:
1. ECDC
   De gegevens van de POWI surveillance en de punt prevalentie surveillance worden periodiek aan het ECDC (Europese Center voor Disease Control) ter beschikking gesteld, in het kader van de Europese surveillances van zorginfecties. Gegevens worden hiervoor gehercodeerd en ziekenhuisnummers worden versleuteld. De gehercodeerde gegevens van de punt prevalentie surveillance worden fysiek opgeslagen bij de ECDC (in TESSy). De gehercodeerde gegevens van de POWI surveillance zijn tot op heden (okt 2019) ook in TESSy opgeslagen. Echter, de POWI gegevens van 2009 t/m 2017 staan daarnaast ook op een beveiligde server binnen het RIVM en zullen binnenkort uit TESSy verwijderd worden. Fysieke opslag van POWI gegevens t.b.v. de ECDC wordt dus vanaf 2018-data alleen binnen het RIVM gerealiseerd. De bedoeling is dat dit in de toekomst ook voor PPS data gaat gebeuren, echter hiervoor is nog geen mogelijkheid gecreëerd.
   Onderzoekers van het ECDC hebben voor hun analyses toegang tot de server zonder dat de gegevens van de server afgehaald kunnen worden.
   Vanuit het ECDC zullen alleen betrokken datamanagers, epidemiologen en onderzoekers toegang hebben tot de data in TESSy.
2. Nethmap
   De antibioticagegevens uit de PPS module worden op persoonsniveau aangeleverd voor het rapport van Nethmap, wat een samenwerkingsverband is tussen het RIVM en de SWAB (Stichting Werkgroep Antibioticagebruik).
3. Externe onderzoekers
   Ziekenhuizen/ZBC's/privéklinieken, universiteiten en andere onderzoeksinstellingen die onderzoek willen doen op de PREZIES data kunnen hiertoe een verzoek indienen bij PREZIES. PREZIES zal dit verzoek beoordelen en bij een positief oordeel zal een

onderzoeksovereenkomst worden gesloten, waarna toegang tot een minimale dataset van gegevens verschaft worden, bij voorkeur binnen de muren van het RIVM.

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Belangen van:

- De Nederlandse maatschappij en overheid (VWS):
  de Nederlandse gemeenschap heeft belang bij inzicht in prevalentie van zorginfecties en de factoren die daar invloed op hebben, zodat we kunnen sturen op beperking van infectiegevallen.
- RIVM:
  Surveillance van infectieziekten met als doel het beschermen van de volksgezondheid. Voldoen aan opdracht vanuit VWS.
- SWAB:
  SWAB heeft belang bij de gegevens over antibioticagebruik om daar onderzoek naar te kunnen doen en te sturen op beheersing van resistentie-ontwikkeling.
- Verwerkers:
  Bedrijfs-/financiële belangen
- Verstrekkers:
  Deelnemende ziekenhuizen/ZBC's/privéklinieken hebben belang bij een overzicht van zorginfecties en risicogegevens binnen hun instelling en het spiegelen van hun eigen infectie- en risicogegevens tegen landelijke cijfers. De resultaten kunnen richtinggevend zijn bij het starten van interventies of aanvullend onderzoek.
- Ontvangers:
  ECDC voert Europese surveillance van zorginfecties uit in het kader van een opdracht voortvloeiend uit de Europese wet. Ook ander externe onderzoekers die gebruik willen maken van de PREZIES data hebben belang bij het inzicht krijgen in trends in, en risico's van, zorginfecties en het effect van interventies, en het feit dat deze data binnen PREZIES al voorhanden is en dus niet opnieuw verzameld hoeft te worden (efficiëntie).

6. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Klik hier om infotekst te verbergen

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch

zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene.

Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

Nederland:
De surveillance wordt uitgevoerd door een netwerk van het RIVM en Nederlandse ziekenhuizen/ZBC's/priveklinieken. Alle gegevensverwerkingen die door het RIVM worden gedaan vinden plaats in Nederland. Ook Relatics BV is in Nederland gevestigd, en hun data wordt in Nederlandse data centers gehost.

(10)(2g)

(10)(2a)

6. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Klik hier om infotekst te verbergen

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;

b. is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
c. berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:
a. wettelijk is toegestaan; en
b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:
- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

RIVM/CIb/EPI - {10)(2e)(10)(2e}, {10)(2e)}

Insturen van surveillancegegevens vindt deels plaats via internetapplicaties en verbindingen op het publieke netwerk. Inloggen gebeurt via inlogcodes, waarbij alleen personen die geverifieerd werkzaam zijn bij één van de betrokken zorginstellingen toegang krijgen. Surveillancegegevens worden ofwel met de hand ingevoerd in OSIRIS, óf er wordt een compleet databestand via een beveiligde email verzonden naar, en verwerkt door, de RIVM datamanagers.
Binnen het RIVM worden gegevens verwerkt en geanalyseerd middels (statistische) programma's zoals Excel, SAS, SPSS, R, stata. RIVM-inlog is hiervoor noodzakelijk.
Zorginstellingen kunnen een rapportage van de ingezonden gegevens opvragen door middel van een internetapplicatie (CIb rapportageomgeving, eigenaar {10)(2e)(10)(2e}, {10)(2e)}, gedelegeerd naar EPI/SIS). De tool die deze rapportages creëert verwerkt de ruwe gegevens tot geaggregeerde data, en spiegelt de gegevens van de zorginstelling aan landelijke geaggregeerde gegevens. Quickscan informatiebeveiliging gemaakt van deze rapportagetool is opvraagbaar bij {10)(2e)} {10)(2e)}.

Gegevens van betrokken contactpersonen en ziekenhuizen worden door het RIVM verwerkt en bijgehouden in Relatics, waarin door medewerkers via een inlogcode ingelogd kan worden.

Er is geen sprake van (semi-) geautomatiseerde besluitvorming, profilering, of big-data verwerkingen.

6. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

- Besluit EU/1082/2013;
- Wet op het RIVM;
- Wet publieke gezondheid (artikelen 3, 6a, 6b, 6c, 28 en 50);
- Wet geneeskundige behandelovereenkomst, artikel 7:458 Burgerlijk Wetboek
- Professionele richtlijnen inzake publieke infectieziektebestrijding waarop de IGZ toeziet: richtlijnen Werkgroep Infectie Preventie: http://www.rivm.nl/Onderwerpen/W/Werkgroep_Infectie_Preventie_WIP/WIP_Richtlijnen.
- Protocollen, gegevensreglement en aanmeldformulieren PREZIES, te vinden op www.prezies.nl.

6. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij **conceptregelgeving** zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij **overheidsverwerkingen** moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.
Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie Persoonsgegeven	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

In het gegevensreglement van PREZIES van 2016 is vastgelegd dat de gegevens voor onbepaalde tijd zullen worden bewaard.
Historische data zijn van belang voor het analyseren en beoordelen van trends over tijd, vandaar dat er momenteel geen data vernietigd worden en hier ook geen plannen voor zijn.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

7. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Klik hier om infotekst te verbergen

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere

onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.
Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

Grondslagen:
Verwerking 1:
- Algemeen belang (artikel 6, lid 1 sub e AVG), en (additioneel vereiste in Unierechtelijk of lidstatelijk recht) :
- Verdragrechtelijke verplichting; deze laatste grondslag is neergelegd in EU Decision 1082/2013, namelijk in artikel 6 lid 3 in combinatie met artikel 2, lid 1 onderdeel a i en ii (surveillance zorginfecties) van dit Europese besluit.
- Lidstatelijk recht: art. 3 lid 1 en 3 Wet RIVM.

Verwerking 2:
- Het RIVM biedt de mogelijkheid om een gepseudonimiseerde code voor de operateur in te voeren in de POWI-module vanwege behoefte van deelnemende organisaties. Die gebruiken de gegevens voor (curatieve) kwaliteitsverbetering. Dat is een gerechtvaardigd belang van de deelnemende organisaties, dus kan het RIVM op basis van artikel 6 lid 1 sub f AVG de gegevens verstrekken, als het belang opweegt tegen de rechten van de betrokkene. In het algemeen kan worden gezegd dat het belang voor kwaliteitsverbetering in curatieve zorg opweegt tegen de privacy van operateurs wat betreft hun relatie tot post-operatieve wondinfecties. In deze specifieke verwerking geldt daarbovenop dat de deelnemende organisaties de gegevens zelf ook al tot hun beschikking hebben en omgekeerd het RIVM de operateur niet kan identificeren zonder extra gegevens (die niet aan het RIVM worden verstrekt). Daarbij is het invoeren van een gepseudonimiseerde code voor de operateur niet verplicht, en maken alleen de organisaties van de mogelijkheid gebruik die de gegevens voor dat belang inzetten.

7. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Klik hier om infotekst te verbergen

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende

uitzonderingen:

a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
b. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
h. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnosen, het verstrekken van gezondheidzorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
j. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

a. wettelijk is toegestaan;
b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij **conceptregelgeving** kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

Verwerking 1: Vanuit de AVG geldt de uitzonderingsgrondslag van artikel 9 lid 2 sub j AVG. De drie onderzoeksmodules vormen wetenschappelijk en/of statistisch onderzoek op grond van Unierecht (artikel 6 lid 3 Besluit 1082/2013/EU) en lidstatelijk recht (artikel 3 lid 1 en 3 Wet op het RIVM) en artikel 24 UAVG.

Verwerking 2: een gepseudonimiseerde code voor de operateur is geen bijzonder gegeven.

8. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij **conceptregelgeving** moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
e. het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een

dergelijk doel te verwerken; en

b. de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.

Er is geen sprake van doelwijziging; de gegevens worden verwerkt t.b.v. surveillance op gebied van zorginfecties.

8. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.
Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het

verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij **conceptregelgeving** kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van het IAK.

a. Proportionaliteit:
de gegevens zijn noodzakelijk voor het uitvoeren van surveillance (zie ook protocollen en gegevensreglement op www.prezies.nl), en worden zoveel mogelijk gepseudonomiseerd. Dataminimalisatie wordt toegepast, waar mogelijk.
Doel van de verwerking van de gegevens is om inzicht en trends in zorginfecties en risicofactoren in kaart brengen om te adviseren over beleid t.a.v. preventie op gebied van zorginfecties in ziekenhuizen en ZBC's in Nederland. Dit is van belang voor de kwaliteit van de Nederlandse volksgezondheid en gezondheidszorg en is daarmee niet onevenredig met de verwerkte persoonsgegevens, mede door hoe de verwerking met waarborgen is omkleed.

b. Subsidiariteit:
Er is geen andere, minder ingrijpende manier om de doeleinden te verwezenlijken. Zonder bijvoorbeeld de infectiegegevens is surveillance minder effectief omdat niet is vast te stellen of er meer of minder dan gemiddeld infecties optreden, en zonder risicofactoren is de surveillance minder effectief omdat het moeilijker of niet is vast te stellen of de infectiegegevens van de instelling daadwerkelijk afwijken van wat verwacht mag worden bij een bepaalde patiëntenpopulatie. Tevens geeft het een indicatie van wat de aandachtspunten zijn in de preventie van infecties.

8. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Klik hier om infotekst te verbergen

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Indien in **conceptregelgeving** een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregelgeving genoemde gronden én moeten specifieke bepalingen

worden opgenomen met betrekking tot ten minste:

a. de verwerkingsdoeleinden;
b. de categorieën van persoonsgegevens;
c. het toepassingsgebied van de ingevoerde beperkingen;
d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
f. de opslagperiodes en de toepasselijke waarborgen;
g. de risico's voor de rechten en vrijheden van betrokkenen;
h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.

Geef bij **overheidsverwerkingen** aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

Indien een betrokkene een beroep wil doen op één van zijn rechten, zal hij dit verzoek schriftelijk (per e-mail of per post) in moeten dienen. Om het verzoek in behandeling te kunnen nemen, moet de identiteit van de verzoeker worden gecontroleerd. De volgende opties zijn mogelijk:

1. Kopie identiteitsbewijs (paspoort, identiteitskaart, rijbewijs, etc.). De verzoeker wordt er op gewezen gebruik te maken van de KopieID app (van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties).
2. Controle identiteit op locatie. Als verzoeker op locatie langskomt, wordt verzoeker gevraagd zijn identiteitsbewijs te tonen en wordt deze gecontroleerd. Een kopie wordt dan niet gemaakt.

Indien de identiteit van de verzoeker is gecontroleerd, wordt het verzoek inhoudelijk getoetst en intern uitgezet. Indien noodzakelijk zal aanvullende informatie worden opgevraagd bij de verzoeker. Binnen vier weken na indiening van het verzoek, wordt in beginsel de verzoeker inhoudelijk geïnformeerd, zodanig dat aan zijn verzoek wordt voldaan. Indien binnen vier weken niet aan het verzoek kan worden voldaan, zal de verzoeker op de hoogte worden gebracht dat de termijn wordt verlengd. Indien het verzoek (deels) wordt afgewezen, wordt dit (binnen de wettelijke termijnen) onderbouwd aan de verzoeker teruggekoppeld.

Specificaties per soort verzoek:

Recht op inzage
Het RIVM verstrekt een overzicht van de persoonsgegevens aan de verzoeker, waarin de volgende informatie staat:

- Of het RIVM persoonsgegevens van de verzoeker verwerkt;
- Wat het doel is van de verwerking;
- Om welke gegevens/categorieën van gegevens het gaat;
- Aan wie het RIVM de gegevens eventueel heeft verstrekt of aan welke categorieën van ontvangers de gegevens zullen worden verstrekt;
- Wat de periode is waarin de persoonsgegevens naar verwachting zullen worden opgeslagen of in elk geval de criteria om die termijn te bepalen;
- Dat de verzoeker verschillende rechten heeft;
- Dat de verzoeker het recht heeft een klacht in te dienen bij de Autoriteit

Persoonsgegevens;
- Wat de herkomst is van de gegevens, als deze bekend is en de gegevens niet bij de verzoeker zijn verzameld;
- Of sprake is van geautomatiseerde besluitvorming inclusief profilering met vermelding van de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor betrokkene.

Recht op correctie
Indien de door het RIVM verwerkte persoonsgegevens niet juist zijn, wijzigt het RIVM de gegevens, worden – indien van toepassing – de organisaties die de oorspronkelijke persoonsgegevens van het RIVM hebben ontvangen, op de hoogte gebracht van de wijziging en worden zij gevraagd deze persoonsgegevens ook te corrigeren en wordt betrokkene van de wijzigingen op de hoogte gesteld.

Recht op verwijdering
Indien het verzoek op verwijdering van persoonsgegevens wordt toegewezen, worden de betreffende persoonsgegevens verwijderd, worden – indien van toepassing – de organisaties die de oorspronkelijke persoonsgegevens van het RIVM hebben ontvangen, op de hoogte gesteld van deze verwijdering en worden zij gevraagd deze persoonsgegevens óók te verwijderen. Daarnaast wordt betrokkene van bovenstaande handelingen op de hoogte gesteld.

Recht op beperking
Indien het verzoek op beperking van de verwerking van persoonsgegevens wordt toegewezen, worden de persoonsgegevens – voor de periode van de beperking – niet verder verwerkt dan gevraagd. Indien van toepassing worden de organisaties die de oorspronkelijke persoonsgegevens van het RIVM hebben ontvangen, op de hoogte gesteld van de beperking en worden zij gevraagd deze persoonsgegevens óók niet verder te verwerken. De betrokkene wordt van de handelingen op de hoogte gebracht.

Recht op bezwaar
Indien het bezwaar van de betrokkene tegen de verwerking van de persoonsgegevens wordt toegewezen, worden de persoonsgegevens niet meer verwerkt. Indien van toepassing worden de organisaties die de oorspronkelijke persoonsgegevens van het RIVM hebben ontvangen, op de hoogte gesteld van het bezwaar en worden zij gevraagd deze persoonsgegevens óók niet meer te verwerken. De betrokkene wordt deze bovenstaande handelingen op de hoogte gebracht.

Recht op dataportabiliteit
Indien het verzoek om persoonsgegevens over te dragen wordt toegewezen, ontvangt betrokkene alle digitale gegevens die de betrokkene zelf actief en bewust heeft verstrekt, de gegevens die de betrokkene indirect heeft verstrekt en de gegevens die zijn verwerkt om een overeenkomst met de betrokkene uit te voeren.

Recht om niet te worden onderworpen aan een uitsluiting op geautomatiseerde verwerking, waaronder profilering
Indien het verzoek wordt toegewezen, zal het RIVM het besluit heroverwegen zonder geautomatiseerde besluitvorming.

Beperkingen van rechten van betrokkenen

Beperkingen van het recht op inzage, rectificatie of beperking van verwerking
Als de persoonsgegevens worden verwerkt voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt, heeft betrokkene geen recht op inzage, recht op rectificatie en recht op beperking van de verwerking en zal het verzoek worden afgewezen. Dit is overeenkomstig art. 44 van de Uitvoeringswet Algemene Verordening

Gegevensbescherming.

Beperkingen van het recht op vergetelheid
In de volgende gevallen heeft betrokkene – overeenkomstig art. 17 Algemene Verordening Gegevensbescherming – geen recht op vergetelheid en zal het verzoek worden afgewezen:

- Als de persoonsgegevens worden verwerkt voor wetenschappelijk onderzoek of statistische doeleinden en als het recht van betrokkene de verwezenlijking van de doeleinden van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
- Als de verwerking nodig is om redenen van algemeen belang op het gebied van volksgezondheid;
- Als de verwerking nodig is voor het nakomen van een wettelijke verplichting.

Beperkingen van het recht op bezwaar
Als de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van een taak van algemeen belang, heeft betrokkene geen recht op bezwaar en zal het verzoek worden afgewezen (art. 21 lid 6 Algemene Verordening Gegevensbescherming).

Overige beperkingen van de rechten van betrokkenen
Als het RIVM persoonsgegevens verwerkt die door het RIVM niet herleidbaar zijn tot een betrokkene, zijn de rechten van betrokkenen niet van toepassing en zal het verzoek worden afgewezen. Dit is overeenkomstig art. 11 van de Algemene Verordening Gegevensbescherming. Een voorbeeld hiervan is als het RIVM gepseudonimiseerde persoonsgegevens verwerkt, waarvan de sleutel bij een andere organisatie ligt. Het RIVM acht het daarnaast ook onevenredig veel inspanning om de gepsuedonimiseerde gegevens te herleiden.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

9. Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Klik hier om infotekst te verbergen

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de

gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:
1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- waar de gegevensverwerking kan leiden tot:
  - discriminatie, stigmatisering en uitsluiting;
  - (blootstelling aan) identiteitsdiefstal of -fraude;
  - financiële verliezen;
  - reputatie- of anderszins relationele schade;
  - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
  - ongeoorloofde ongedaanmaking van pseudonimisering;
  - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of

- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.
Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:
- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen.
Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

a.	Als herleidbare gegevens over gezondheid op straat zouden komen te liggen, is dit uiteraard zeer ernstig. Dit zou kunnen leiden tot discriminatie, stigmatisering of uitsluiting (zoals moeite met het vinden van werk, problemen met (zorg)verzekeraars), en schade wat betreft reputatie en/of relatie. Daarnaast kan het leiden tot gevoelens van stress of angst bij de betrokkene, of verlies van vertrouwen in het medisch

beroepsgeheim.
Gegevens die PREZIES verzamelt over contactpersonen zijn gewone persoonsgegevens waaruit geen gegevens over gezondheid of (seksueel) gedrag uit zijn af te leiden.

b. Een denkbaar risico bestaat uit een datalek bv via
- een opgeslagen bestand op een USB-stick,
- een onbeveiligde mail naar een verkeerd mailadres,
- onjuist geadresseerde of bezorgde post,
- documenten die niet achter slot en grendel bewaard worden en in handen komen van een onbevoegd persoon,
- een onbevoegd persoon die toegang heeft tot digitale databestanden,
- kwade wil van binnenuit (boze werknemers die bewust lekken of sleutels vrijgeven), of
- kwade wil van buitenaf (hackers).

→ denkbare risico's:
1) Doorbreken van de pseudonimisatie (vrijgeven van algoritme of code), of onjuist toepassen van pseudonimisatie, door de deelnemende zorginstellingen,
2) Doorbreken van de codering van ziekenhuizen (zie voorbeeld beschreven onder a),
3) Opslag op TESSy server: POWI en PPS gegevens van 2017 en eerder zijn reeds ingezonden naar de ECDC en staan aldaar opgeslagen op de TESSy server. In principe vallen deze gegevens onder de Europese wetgeving en zijn daarom potentieel door een ieder op te vragen via een beroep op de openbaarheid van bestuur. Tot nu toe heeft dit in Europees verband nog niet plaatsgevonden, en het is dus niet met zekerheid te zeggen of gegevens dan aan de aanvrager overhandigd zullen moeten worden of niet. Vooruitlopend hierop zijn alle vanaf 2009 door Nederland aangeleverde gegevens over de surveillance van POWI's recent op een beveiligde server binnen het RIVM geplaatst, van waaruit ze bereikbaar zijn voor de ECDC voor analyses maar niet te downloaden zijn en formeel daarmee niet meer onder de ECDC vallen. Op korte termijn zullen de gegevens die op deze server zijn geplaatst verwijderd worden uit TESSy, waardoor deze dan niet meer op te vragen zullen zijn via de Europese regelgeving v.w.b. wet openbaarheid bestuur. Voor POWI-gegevens van vóór 2009 wordt deze exercitie niet verricht, en voor gegevens uit het PPS is momenteel nog geen technische mogelijkheid om van deze zgn. "remote access" mogelijkheid gebruik te maken.
4) WOB-verzoek: Ook in Nederland zouden de gegevens van PREZIES opgevraagd kunnen worden d.m.v. een beroep op de WOB. Dit is in het verleden één keer eerder gebeurd, waarna na een gang naar de rechter PREZIES de gegevens niet hoefde te delen. Of de argumenten die destijds golden in deze tijd nog steeds stand zouden houden is niet met zekerheid te zeggen.
5) insturen data door zorginstellingen via onbeveiligde mail: alhoewel PREZIES alleen data via beveiligde mail verstuurt naar zorginstellingen en PREZIES de zorginstellingen ook met nadruk verzoekt om voor het verzenden van bestanden met patiëntgegevens alleen van beveiligde mail gebruik te maken, doen niet alle zorginstellingen dit.

c. De kans dat deze gevolgen zullen optreden is klein. Voor zover bekend heeft er nog nooit een dergelijk datalek vanuit RIVM/CIb/EPI plaatsgevonden. Bovendien gaat het v.w.b. patiëntgegevens binnen PREZIES altijd om gepseudonimiseerde gegevens, waarbij zonder sleutel de herleidbaarheid tot een individu redelijkerwijs niet mogelijk is. Als deze gegevens op straat zouden komen te liggen is dit uiteraard ernstig maar zijn deze gegevens daardoor niet direct herleidbaar. De gegevens zijn alleen herleidbaar te maken indien iemand de pseudonimisatie weet te doorbreken door allereerst de codering van het ziekenhuisnummer te ontcijferen, en vervolgens in de desbetreffende zorginstelling in het ziekenhuisinformatiesysteem inlogt en gaat zoeken op gegevens

zoals geboortedatum, geslacht etc.
Voor de applicatie Osiris geldt voor gebruikers geen verplichting om regelmatig het wachtwoord te veranderen. Er is geconstateerd dat sommige gebruikers al jaren hetzelfde wachtwoord hanteren. Hierdoor bestaat ook het risico dat er accounts bestaan die niet meer actief (horen te) zijn.

d. De impact voor de betrokkenen hangt af van de aard van de gegevens, en of deze herleidbaar zijn naar een individu.
In het geval van de PREZIES gegevens zijn deze niet eenvoudig herleidbaar naar een individu, zie ook onder punt a en c toegelicht.

Voor medewerkers van PREZIES en andere RIVM medewerkers (bijv SSC- CAMPUS) geldt een geheimhoudingsplicht, zoals vastgesteld voor ambtenaren.
Sinds de inrichting van de surveillancesystemen in de vorige eeuw heeft zich een dergelijk risico met negatieve gevolgen niet gerealiseerd. De kans op een incident moet als zeer klein worden ingeschat. De technische en organisatorische beveiligingsmaatregelen worden op dit moment weer opnieuw doorgelicht en up-to-date gebracht.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

10. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Klik hier om infotekst te verbergen

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.
Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.
Ter illustratie noemt de AVG de volgende maatregelen:

a. pseudonimiseren en versleutelen van persoonsgegevens;
b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;

- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

a. controle op de toegang tot de apparatuur;
b. controle op de gegevensdragers;
c. opslagcontrole;
d. gebruikscontrole
e. controle op de toegang tot gegevens;
f. transmissiecontrole;
g. invoercontrole;
h. transportcontrole; en
i. herstelmogelijkheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegevens in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Technische maatregelen:

- Pseudonimiseren van persoonsgegevens aan de bron
- Toegangscontrole op wie het RIVM-terrein op mag, inloggen in SSC Campus via inlognaam en wachtwoord
- Data invoer en opslag in OSIRIS: Osiris is een webapplicatie waarbij toegang alleen geregeld wordt door middel van een wachtwoord. In Osiris worden gegevens van cliënten opgeslagen, die zeer vertrouwelijk zijn. Aan de beveiliging van deze gegevens worden hoge eisen gesteld. De verwerking van gezondheidsgegevens via internet mag volgens de Autoriteit Persoonsgegevens alleen met behulp van (minimaal) meerfactorauthenticatie. Zie o.a. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen. Dit is momenteel nog niet geregeld, maar aan het in gebruik nemen van 2 factor-authentificatie wordt momenteel wel gewerkt en zal naar verwachting eind mei 2020 op deze data worden toegepast.
- De bestanden met bijzondere persoonsgegevens, die zich bevinden op de R-schijf, zijn beveiligd door slechts een beperkt aantal personen (PREZIES-medewerkers en PREZIES-datamanagers) toegang te verschaffen tot de map (rechten toe te kennen). Uitgezocht kan nog worden of dit in alle gevallen goed is ingesteld en ook naar behoren werkt.
- 2 factor-authenticatie in geval van inloggen in Campus buiten het RIVM
- Regelmatige controle op wie toegang heeft tot Osiris en bijbehorende rechten (proces wordt gestart om dit elke 6 maanden te kunnen controleren).
- Bewaren van gevoelige documenten achter slot en grendel.
- Het opvragen van cliënt gegevens in zorginstellingen gebeurt beveiligd, bijvoorbeeld door gebruik van Filesender of Zorgmail.
- De data zijn opgeslagen in Osiris. De deelnemende zorginstellingen hebben toegang tot hun eigen data middels een gebruiksnaam en wachtwoord, bij het maken van aanpassingen wordt een nieuwe melding opgeslagen waarbij wordt bijgehouden wie deze melding heeft gemaakt. De onderzoekers binnen het RIVM hebben toegang tot de data van alle zorginstellingen.

Organisatorische maatregelen:

- Dataminimalisatie in de gehele keten als uitgangspunt
  - Overwegen/bespreken of de variabelen 'wondklasse' en 'vervolgOK' uit het protocol van de punt prevalentie surveillance verwijderd kunnen worden.
  - Overwegen/bespreken of de 7-letterige code voor aanduiding van de chirurg uit het protocol van de POWI-surveillance verwijderd kan worden.
- Toegang tot databestanden alleen voor betrokken onderzoekers
- Periodieke audits vinden intern plaats.
- Indien verzending per post: zo weinig mogelijk persoonsgegevens meesturen
- Computer op lock zetten bij afwezigheid

Juridische maatregelen:

- Vastleggen van overeenkomsten indien nodig/wenselijk (verwerkersovereenkomsten, samenwerkingsovereenkomsten)
- Het vastleggen van de bovengenoemde technische en organisatorische maatregelen in dienstverlenings- en verwerkersovereenkomsten met verwerkers en in overeenkomsten met de betrokken zorginstellingen (o.b.v. jaarlijkse aanmeldformulieren);
- Het vastleggen in verwerkersovereenkomsten van de in artikel 23, tweede lid, van de Uitvoeringswet AVG, vereiste geheimhoudingsplicht van de verwerkers;
- Het vastleggen in overeenkomsten van de verplichting voor de verwerkers om te voldoen aan de Baseline Informatiebeveiliging Rijksdienst (BIR);
- De wettelijk vastgelegde voorwaarde uitsluitend gegevens te verwerken onder medisch beroepsgeheim, ambtelijke geheimhoudingsplicht dan wel contractueel vastgelegde

opdracht tot geheimhouding.

Hier kunt u aanvullende punten toevoegen: selecteer de tab *Invoegen*, kies *Snelonderdelen, Aanvullend punt*

Voeg hier wanneer gewenst een afsluitende alinea toe. Denk bijvoorbeeld aan:

- Lessen uit deze PIA
  - De beveiliging van de PREZIES gegevens is zo veilig als de zwakste schakel. In deze surveillance hebben we voor wat betreft de patiëntengegevens te maken met zorginstellingen, het RIVM en de ECDC. Als het RIVM alles netjes beveiligt maar de zorginstellingen gebruiken geen gepseudonimiseerde patiëntidentifier (verplicht, zoals gecommuniceerd via het protocol), of de zorginstellingen versturen de data niet via een beveiligde verbinding zoals aangegeven, dan hebben alle maatregelen van het RIVM weinig of in ieder geval minder nut. Dit geldt ook voor de samenwerking met de ECDC. Daarom zijn we afgelopen jaar overgestapt naar het bewaren van de gegevens voor de ECDC op een op het RIVM gestalde server. Op deze manier vallen de gegevens altijd onder de Nederlandse wetgeving en zijn we niet afhankelijk van de Europese wetgeving en hoe het ECDC de WOB-verzoeken afhandelt.
- Volgende stappen
  - Ontwikkelen 2-factor authentificatie voor inloggen in Osiris en controleren of er autorisaties
  - Verwijderen surveillancedata uit TESSy zodra deze voor ECDC beschikbare data is opgeslagen op de speciaal hiervoor ingerichte beveiligde server binnen het RIVM.

Per surveillancesysteem een alinea toevoegen:
Geef aan welke maatregelen nog nodig zijn, en welke andere lessen/actiepunten uit deze PIA naar voren komen.


Maatregelen
nemen
Privacybewustwording
Doelbinding
PIA
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier