GEBRUIKSVOORWAARDEN

PHILIPS INTEROPERABILITY SOLUTIONS PORTAAL

Versie 27 Juli 2020

Wij verzoeken u vriendelijke de onderstaande Gebruiksvoorwaarden grondig door te nemen.

1. **Algemeen:**

   - Forcare Holding B.V., een dochteronderneming van Koninklijke Philips N.V. (hierna: "Philips"), heeft in het kader van de bestrijding van het COVID-19 virus een gratis online portaal ingericht (hierna: het Portaal).
   - In het Portaal kan een ziekenhuis handmatig informatie invoeren over een patiënt. Vervolgens kan het ziekenhuis toestemming geven aan individuele ziekenhuizen om de informatie van de betreffende patiënt te bekijken.
   - Ook kan het Portaal worden gebruikt om radiologische studies van het ene ziekenhuis door radiologen van een ander ziekenhuis te laten beoordelen, waarna de verslagen via het Portaal terug naar het eerste ziekenhuis kunnen worden gestuurd.
   - Op deze manier kunnen ziekenhuizen in Nederland eenvoudig informatie uitwisselen over een patiënt die van het ene ziekenhuis wordt overgebracht naar het andere ziekenhuis. Het doel van het Portaal was de verdeling van Corona-patiënten over het land te faciliteren.
   - Ter voorbereiding op een eventuele tweede uitbraak van het COVID-19 virus, zal het Portaal tot 31 december 2020 beschikbaar blijven. Het Portaal mag thans worden gebruikt voor alle patiëntverwijzingen; ook voor niet COVID-19 gerelateerde patiëntenzorg.
   - Deze Gebruiksvoorwaarden zijn van toepassing op het gebruik van het Portaal door het ziekenhuis. Door het aanvaarden van deze Gebruiksvoorwaarden en/of het in gebruik nemen van het Portaal, stemt het ziekenhuis in met deze Gebruiksvoorwaarden en aanvaardt het ziekenhuis dat zij gebonden is aan deze Gebruiksvoorwaarden.
   - Philips behoudt zich het recht voor deze Gebruiksvoorwaarden tussentijds te wijzigen. Het ziekenhuis wordt actief op de hoogte gebracht van eventuele herziene versies van de Gebruiksvoorwaarden en deze zullen in het Portaal worden gepubliceerd. Mocht het ziekenhuis niet akkoord zijn met de nieuwe Gebruiksvoorwaarden, dan kan zij het gebruik van het Portaal beëindigen.
   - Philips behoud zich eveneens het recht voor het Portaal te wijzigen en eventuele functies toe te voegen of te verwijderen, dan wel het gebruik van het Portaal geheel (of gedeeltelijk) te beëindigen, waaronder (doch niet uitsluitend) indien de COVID-19 epidemie is geëindigd of het Portaal niet langer nuttig wordt geacht door het verloop van de epidemie (zie hierna ook "Einde van het gebruik").
   - Deze Gebruikersvoorwaarden zullen mede van toepassing zijn op eventuele nieuwe functies.

2. **Gebruik van het Portaal**:

   - Voor het gebruik van het Portaal is benodigd:
     - acceptatie van deze Gebruiksvoorwaarden;

- aanmelding bij Philips van twee "key users" per ziekenhuis middels het daarvoor bestemde aanmeldformulier, die vervolgens meerdere gebruikers kunnen (laten) aanmaken;
- een account met inloggegevens voor de gebruikers van het ziekenhuis, waarmee kan worden ingelogd op het Portaal;
- een verbinding met internet; en
- een mobiel telefoonnummer voor iedere gebruiker van het ziekenhuis, voor het ontvangen van een verificatiecode.

- Het Portaal wordt gratis aan Nederlandse ziekenhuizen ter beschikking gesteld. Het kan echter zo zijn dat wordt besloten bepaalde aanvullende functionaliteiten tegen betaling beschikbaar te stellen. Het ziekenhuis zal worden geïnformeerd als functionaliteiten tegen betaling beschikbaar zullen worden gesteld. In dat geval heeft het ziekenhuis de mogelijkheid deze betaalde functionaliteiten af te nemen tegen de toepasselijke vergoeding dan wel het gebruik van het Portaal te beëindigen.
- Het ziekenhuis is zelf verantwoordelijk voor het beschermen van de inloggegevens van haar gebruikers en ervoor te zorgen dat alleen bevoegde personen gebruik kunnen maken van het Portaal. Wij raden het ziekenhuis aan haar gebruikers te instrueren hun inloggegevens geheim te houden en met niemand te delen.
- Het ziekenhuis is zelf verantwoordelijk voor de informatie die in het Portaal wordt ingevoerd en het beschikbaar houden/bewaren/opslaan van de informatie buiten het Portaal. Daarnaast is het ziekenhuis verantwoordelijk voor het tijdig verwijderen van de door haar ter beschikking gestelde informatie en (waar nodig) het corrigeren van onjuiste informatie.
- Het ziekenhuis heeft de mogelijkheid haar gegevens in het Portaal te verwijderen en/of te corrigeren.

3. <u>(Ongeoorloofd) gebruik</u>:

- Het Portaal mag door het ziekenhuis of haar gebruikers niet worden gebruikt op een illegale of oneerlijke manier. Ook mogen het ziekenhuis en haar gebruikers het Portaal niet gebruiken op een manier die anderen schade toebrengt. Daarom zijn in ieder geval de volgende handelingen (of pogingen daartoe) verboden:
  - het omzeilen of verwijderen van de beveiliging van het Portaal;
  - het kopiëren, nabouwen of inbouwen in de eigen website of (mobiele) applicatie van het Portaal;
  - het gebruiken van het Portaal om geld te verdienen, bijvoorbeeld door het Portaal aan anderen in gebruik te geven;
  - het vullen van het Portaal met niet patiënt gerelateerde informatie of auteursrechtelijke beschermde teksten of foto's van derden, als het ziekenhuis daarvoor niet eerst de toestemming van die anderen heeft gekregen;
  - het gebruiken van het Portaal voor strafbare of anderszins onrechtmatige activiteiten;
  - het gebruiken van het Portaal om virussen of andere malware te verspreiden;
  - het gebruiken van het Portaal om anderen te misleiden; en

- het geven van inloggegevens aan anderen of het op enige andere wijze delen van of toegang geven tot het Portaal aan derden of anderszins onbevoegde personen.

4. **Einde van het gebruik:**

- Philips kan het gebruik van het Portaal door het ziekenhuis of dat van haar gebruiker(s) tijdelijk of permanent beëindigen in het geval:
  - er reden is te twijfelen aan de identiteit van degene die gebruik maakt van het Portaal (er is bijvoorbeeld een redelijk vermoeden dat degene die het Portaal gebruikt niet degene is die de inloggegevens oorspronkelijk heeft ontvangen);
  - er reden is te twijfelen aan de acceptatie en/of naleving van deze Gebruiksvoorwaarden door het ziekenhuis.
- Het Portaal kan door het ziekenhuis tot 31 december 2020 kosteloos worden gebruikt. Per 1 januari 2021 eindigt de licentie voor het gebruik van het Portaal van rechtswege en dient het gebruik van het Portaal door het ziekenhuis te worden gestaakt.
- Het ziekenhuis kan zelf het gebruik van het Portaal te allen tijde beëindigen waarna Philips haar account op haar verzoek zal verwijderen.
- Nadat het gebruik van het Portaal is geëindigd, kan het ziekenhuis Philips binnen dertig dagen verzoeken haar gegevens uit het Portaal aan haar te retourneren dan wel te verwijderen. Indien dit verzoek niet binnen dertig dagen na beëindiging van het gebruik door Philips is ontvangen, behoudt Philips zich het recht voor de gegevens definitief te verwijderen.
- Vanaf 31 december 2020 zal het Portaal onderdeel gaan uitmaken van de bestaande (betaalde) interoperabiliteitsplatform van Philips. Mocht het ziekenhuis na 31 december 2020 gebruik willen maken van het Portaal als onderdeel van deze dienstverlening, dan kan zij daarvoor op vrijwillige basis een separate overeenkomst sluiten met Philips.

5. **Beveiligingsmaatregelen:**

- Om de veiligheid van de (medische) gegevens van het ziekenhuis te waarborgen, zijn door Philips verschillende beveiligingsmaatregelen getroffen.
- Om in te kunnen loggen op het Portaal dienen de gebruikers in de eerste plaats een gebruikersnaam en wachtwoord in te voeren. Daarnaast dient de gebruiker een eenmalige unieke (tweede) authenticatie factor in te voeren. Alleen als deze twee stappen succesvol zijn doorlopen, krijgt de gebruiker toegang tot het Portaal.
- Voorts voldoet de beveiliging van het Portaal aan de NEN7510, NEN7512, NEN7513 en ISO27001 standaarden.

6. **Privacy:**

- Het ziekenhuis is verwerkingsverantwoordelijke met betrekking tot de door haar in het kader van het Portaal verwerkte persoonsgegevens. Philips is verwerker in relatie tot de ziekenhuizen die gebruik maken van het Portaal. Philips en het ziekenhuis bevestigen hierbij dat ieder zal voldoen aan alle op haar van toepassing zijnde wettelijke voorschriften betreffende de te verwerken persoonsgegevens, daaronder in het bijzonder begrepen de voorschriften bij of krachtens de Algemene Verordening Gegevensbescherming (AVG). Op de verwerking van persoonsgegevens door Philips zijn voorts de voorwaarden van de onderstaande Verwerkingsovereenkomst van toepassing (zie hieronder).

7. **Geheimhouding:**

- Philips zal alle informatie en/of gegevens die zij in het kader van (de uitvoering van) deze Gebruiksvoorwaarden verkrijgt, geheimhouden en niet zonder schriftelijke toestemming van het ziekenhuis aan derden - met uitzondering van derden die door haar bij de uitvoering van de Gebruiksvoorwaarden worden ingeschakeld - bekend maken, tenzij bekendmaking geschiedt op grond van een wettelijke verplichting of rechterlijk bevel.
- De geheimhoudingsverplichtingen zoals genoemd in dit artikel hebben geen betrekking op:
  a) informatie/gegevens die op het moment dat deze ter beschikking kwam van Philips reeds voor het publiek toegankelijk was;
  b) informatie/gegevens die nadat deze ter beschikking kwam van Philips voor het publiek toegankelijk is geworden, tenzij dit het gevolg is van het niet nakomen door Philips van haar verplichtingen uit hoofde van dit artikel; of
  c) informatie/gegevens die Philips op rechtmatige wijze heeft verkregen c.q. daarmee bekend is geworden voordat deze informatie/gegevens aan Philips ter beschikking werd gesteld.
- Philips verplicht zich jegens ziekenhuis om de verplichtingen zoals genoemd in voorgaand lid van dit artikel op te leggen aan degenen die (waaronder begrepen werknemers van Philips) namens Philips belast zijn met de uitvoering van de Gebruiksvoorwaarden en staat er jegens ziekenhuis voor in dat deze personen deze verplichtingen nakomen.

8. **Intellectuele eigendomsrechten:**

- De intellectuele eigendomsrechten, waaronder auteursrechten en databankrechten, ten aanzien van het Portaal en eventuele wijzigingen daarvan zijn en blijven eigendom van Philips. Dat betekent dat derden niet zonder toestemming van Philips het Portaal mogen gebruiken, aan welke toestemming Philips voorwaarden kan verbinden.
- Als het ziekenhuis en/of haar gebruikers een opmerking, suggestie of andere informatie indienen bij Philips over het Portaal (hierna: "Feedback"), dan dragen zij op dat moment de eigendom op die Feedback over aan Philips. Philips mag de Feedback dan gebruiken en implementeren zoals zij dat wil. Uiteraard waardeert Philips alle Feedback, maar ze zal daarvoor geen vergoeding betalen.

9. **Aansprakelijkheid:**

- Uiteraard doet Philips haar uiterste best het Portaal steeds beschikbaar en online te houden. Philips kan echter niet garanderen dat het Portaal altijd beschikbaar is en dat het zonder fouten of onderbrekingen functioneert. Philips verstrekt ook anderszins geen garanties met betrekking tot het Portaal.
- Philips is in geen geval verantwoordelijk voor 1) de inhoud van de (medische) gegevens die door de gebruikers worden ingevoerd of opgevraagd; en 2) de manier waarop het Portaal door het ziekenhuis wordt gebruikt.
- Philips is niet aansprakelijk voor door het ziekenhuis en/of derden geleden schade of gemaakte kosten in verband met het Portaal, behoudens aansprakelijkheid voor (i) overlijden of persoonlijk letsel; en (ii) schade veroorzaakt door opzet, bedrog of grove nalatigheid.

10. **Klachten en/of vragen:**

- Ondanks de zorg die Philips heeft besteed aan de ontwikkeling van het Portaal, kunnen fouten of onvolkomenheden bestaan of optreden. Mocht het ziekenhuis fouten of

onvolkomenheden ontdekken of een andere vraag of klacht hebben over het functioneren van het Portaal, dan kan zij contact opnemen met Philips via [redacted]@philips.com. Vervolgens zullen de klachten en/of vragen zo snel als redelijkerwijs mogelijk is in behandeling worden genomen door Philips.

11. <u>Slotbepalingen:</u>

- Op deze Gebruiksvoorwaarden is Nederlands recht van toepassing. Eventuele geschillen in verband met of voortvloeiend uit deze Gebruiksvoorwaarden zullen worden voorgelegd aan de bevoegde rechter van de rechtbank Amsterdam.
- Het ziekenhuis bevestigt dat zij in Nederland gevestigd is en dat zij niet, direct of indirect, het Portaal zal (her)exporteren naar een ander land of vanuit een ander land gebruik zal maken van het Portaal.

***

Verwerkersovereenkomst

gebaseerd op de BOZ versie 121217

Algemeen

- Deze Verwerkersovereenkomst maakt onderdeel uit van de "Gebruikersvoorwaarden Interoperability Solutions Portaal" en zijn van toepassing op ieder gebruik van het Portaal van Forcare Holding B.V. ("Philips").

- Philips wordt hierna ook wel aangeduid als "**Verwerker**" en het ziekenhuis als "**Verwerkingsverantwoordelijke**". Ieder van hen wordt hierna ook wel aangeduid als "**Partij**" of gezamenlijk als "**Partijen**".

Artikel 1. Definities

1.1. In deze Verwerkersovereenkomst wordt onder de volgende met een hoofdletter aangeduide begrippen het volgende verstaan:

a)	Algemene Verordening Gegevens Bescherming of AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
b)	Betrokkene	een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).

c)	Binding Corporate Rules for Processors	Een wereldwijd beleid en raamwerk van Verwerker met betrekking tot de verwerking van persoonsgegevens in gevallen waar Verwerker of een van haar zustermaatschappijen optreedt als Verwerker of subverwerker. Deze zijn goedgekeurd door de relevante EU Autoriteiten Persoonsgegevens in het licht van artikel 26 (2) van Richtlijn 95/46/EG en geratificeerd in artikel 47 van de AVG, om de wereldwijde gegevensverwerking in opdracht van opdrachtgevers binnen de groepsmaatschappijen waarvan Verwerker deel uitmaakt mogelijk te maken.
d)	Derde	een derde als bedoeld in artikel 4 sub 10 AVG.
e)	Functionaris voor de Gegevensbescherming	een functionaris als bedoeld in artikel 37 e.v. AVG.
f)	Incident	i een klacht of (informatie)verzoek van een Betrokkene met betrekking tot de verwerking van Persoonsgegevens door Verwerker; ii een onderzoek naar of beslaglegging door overheidsfunctionarissen op de Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden; iii een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 onder 12 AVG; iv iedere ongeautoriseerde toegang, verwijdering, verminking, verlies of enige andere vorm van onrechtmatige verwerking van de Persoonsgegevens.
g)	Medewerker	de door Partijen voor de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen.
h)	Overeenkomst(en)	de in Bijlage 1 vermelde overeenkomst(en) betreffende de levering van producten en/of diensten.
i)	Partij	Verwerkingsverantwoordelijke of Verwerker.

j)	Partijen	Verwerkingsverantwoordelijke en Verwerker.
k)	Persoonsgegeven	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van artikel 4 onder 1 AVG.
l)	Subverwerker	iedere niet-ondergeschikte derde partij die door Verwerker is betrokken bij de verwerking van Persoonsgegevens in het kader van de Overeenkomst, niet zijnde Medewerkers.
m)	Verwerker	de verwerker als bedoeld in artikel 4 sub 8 AVG
n)	Verwerkersovereenkomst	de onderhavige overeenkomst.
o)	Verwerkingsverantwoordelijke	de verwerkingsverantwoordelijke als bedoeld in artikel 4 sub 7 AVG
p)	Wet bescherming persoonsgegevens of Wbp	Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), inclusief latere wijzigingen.

1.2. Voornoemde en overige begrippen worden geïnterpreteerd overeenkomstig de AVG. Tot aan 25 mei 2018 worden begrippen geïnterpreteerd overeenkomstig de vergelijkbare bepaling uit de Wbp.

1.3. Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN7510) wordt daarmee steeds gedoeld op de meest actuele versie daarvan.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst

2.1. Deze Verwerkersovereenkomst heeft betrekking op de verwerking van Persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst(en).

2.2. Partijen sluiten de Overeenkomsten voor de in de Overeenkomsten beschreven doeleinden. Verwerker staat ervoor in dat hij ook expertise heeft wat betreft de in deze Verwerkersovereenkomst beschreven gegevensbescherming in het kader van de uitvoering van de in de Overeenkomsten beschreven dienstverlening.

2.3. Deze Verwerkersovereenkomst maakt onverbrekelijk deel uit van de Overeenkomst(en). Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Overeenkomst(en), prevaleert het bepaalde in de Verwerkersovereenkomst.

Artikel 3. Uitvoering verwerking

3.1. Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend Persoonsgegevens zal verwerken voor zover:

a.) dit noodzakelijk is voor de uitvoering van de Overeenkomst (binnen de kader als gespecificeerd in Bijlage 1); of

b.) Verwerkingsverantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven;

3.2. In het kader van het bepaalde in het eerste lid van artikel 3 onder a) zal Verwerker uitsluitend de in Bijlage 1 gespecificeerde Persoonsgegevens verwerken in het kader van de in die bijlage beschreven aard en doeleinden van de verwerking.

3.3. Verwerker zal alle redelijke en tijdig gegeven instructies van Verwerkingsverantwoordelijke in verband met de verwerking van Persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van Persoonsgegevens.

3.4. Onverminderd het bepaalde in het eerste lid van dit artikel 3, is het Verwerker toegestaan om Persoonsgegevens te verwerken als een wettelijk voorschrift (waaronder ook begrepen daarop gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren en de verplichte verwerking beperken tot het strikt noodzakelijke.

3.5. Verwerker zal de Persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de AVG en overige wet- en regelgeving. Verwerker zal in dat kader ten minste een register van verwerkingen aanleggen als bedoeld in artikel 30 AVG en op eerste verzoek van Verwerkingsverantwoordelijke een kopie van dat register verstrekken, voor zover toeziend op de verwerking van Persoonsgegevens in het kader van de onderhavige Verwerkersovereenkomst.

3.6. Vervalt.

3.7. Voor de uitvoering van de Overeenkomst(en) en deze Verwerkersovereenkomst is het mogelijk dat Verwerker subverwerkers en groepsvennootschappen dient in te zetten, die mogelijk zijn gevestigd buiten de EER (alle huidige lidstaten van de Europese Unie, Noorwegen, IJsland, Liechtenstein en Zwitserland).

Intra groep doorgiften: De bindende bedrijfsvoorschriften of binding corporate rules van Verwerker ("BCR's") en de aanvullende bepalingen van dit artikel zijn van toepassing op het verwerken van Persoonsgegevens namens Verwerkingsverantwoordelijke, indien zulke Persoonsgegevens (i) zijn onderworpen aan de beperkingen voor het doorgeven van Persoonsgegevens zoals opgenomen in de BCR's en (ii) door Verwerker worden verwerkt in een land zonder adequate bescherming van persoonsgegevens (zoals gedefinieerd in de BCR's). De laatste versie van de BCR's is te vinden op de Verwerker's website. De BCR's maken een integraal onderdeel uit van deze Verwerkersovereenkomst.

Verwerker spant zich ervoor in om de EU-goedkeuring van de BCR's in stand te houden en uit te breiden voor de duur van deze Verwerkersovereenkomst en Verwerkingsverantwoordelijke spoedig ervan op de hoogte te brengen indien er een materiële wijziging is in de EU goedkeuring van de BCR's.

Doorgiften naar derde partijen: Verwerker draagt er voor zorg dat een doorgifte van Persoonsgegevens naar enige subverwerker van Verwerker die geen groepsvennootschap is, plaatsvindt onder een geldige grondslag voor doorgifte naar derde landen zoals benoemd in Hoofdstuk V van de AVG.

3.8. Verwerker waarborgt dat betrokken Medewerkers zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

Artikel 4. Beveiliging Persoonsgegevens en controle

4.1. Verwerker zal aantoonbaar, passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de (in Bijlage 1 gespecificeerde) aard van de te verwerken Persoonsgegevens, ter bescherming van de Persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen. In deze beveiligingsmaatregelen zijn de mogelijk in de Overeenkomst reeds bepaalde maatregelen begrepen. De maatregelen omvatten in ieder geval:

a.) maatregelen om te waarborgen dat enkel bevoegde Medewerkers toegang hebben tot de Persoonsgegevens voor de doeleinden die zijn uiteengezet;

b.) maatregelen waarbij de Verwerker zijn Medewerkers en Subverwerkers uitsluitend toegang geeft tot Persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die Persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;

c.) maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

d.) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan Verwerkingsverantwoordelijke;

e.) maatregelen om de tijdige beschikbaarheid van de Persoonsgegevens te garanderen;

f.) maatregelen om te waarborgen dat Persoonsgegevens logisch gescheiden worden verwerkt van de Persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt;

g.) de overige maatregelen die Partijen zijn overeengekomen zoals vastgelegd in Bijlage 2.

4.2. Verwerker werkt aantoonbaar in overeenstemming met ISO27001 en/of NEN 7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van Persoonsgegevens, waarin in ieder geval de in het eerste lid van dit artikel 4 genoemde maatregelen uiteen zijn gezet.

4.3. Verwerker voldoet aantoonbaar aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN7512.

4.4. Verwerker voldoet aantoonbaar aan de eisen ten aanzien van logging zoals beschreven in NEN7513.

4.5. Vervalt.

4.6. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen, indien deze daarover beschikt, waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

4.7. Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder 4.1 t/m 4.4 genoemde maatregelen. Verwerker stelt

Verwerkingsverantwoordelijke, indien Verwerkingsverantwoordelijke daarom verzoekt, hiertoe met redelijke tussenpozen, maar niet vaker dan éénmaal per jaar en voorts in de situaties zoals beschreven in artikel 5 van deze Verwerkersovereenkomst, in de gelegenheid om op kosten van Verwerkingsverantwoordelijke, op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip, door Verwerkingsverantwoordelijke of een door Partijen in gezamenlijk overleg aan te wijzen derde partij, zulks te (laten) controleren. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijke controle in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen. Alle auditrapporten en -materialen zullen door Partijen vertrouwelijk worden behandeld en niet aan derden worden geopenbaard.

4.8. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel 4. Het voorgaande laat de instructiebevoegdheid van Verwerkingsverantwoordelijke om zo nodig aanvullende maatregelen te (doen) treffen onverlet.

Artikel 5. Monitoring, informatieplichten en incidentenmanagement

5.1. Verwerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan Verwerkingsverantwoordelijke.

5.2. Zodra Verwerker een Incident ontdekt, is Verwerker verplicht Verwerkingsverantwoordelijke daarvan onverwijld in kennis te stellen en daarbij alle relevante informatie te verstrekken omtrent:

1) de aard van het Incident,
2) de getroffen gegevens,
3) de geconstateerde en de vermoedelijke gevolgen van het Incident, en
4) de maatregelen die getroffen zijn of zullen worden om het Incident op te lossen dan wel de gevolgen/schade zo veel mogelijk te beperken.

5.3. Verwerker is verplicht in geval van een Incident om passende maatregelen te nemen om de gevolgen/schade waar mogelijk zo veel mogelijk te beperken en in de toekomst te voorkomen. Waar mogelijk treedt Verwerker in overleg met Verwerkingsverantwoordelijke. Als de aard van het Incident vereist dat Verwerker onmiddellijk handelt, vindt dit overleg achteraf plaats.

5.4. Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen bij het verstrekken van informatie en de redelijke instructies van Verwerkingsverantwoordelijke opvolgen, met als doel Verwerkingsverantwoordelijke in staat te stellen een deugdelijk onderzoek te verrichten naar het Incident, een correcte respons te formuleren en in onderling overleg passende vervolgstappen te nemen ten aanzien van het incident, waaronder begrepen het informeren van de AP en/of de betrokkene zoals bepaald in artikel 5.8.

5.5. Verwerker zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Verwerkingsverantwoordelijke van een onmiddellijke reactie over een Incident te voorzien, en om effectief samen te werken met Verwerkingsverantwoordelijke om het Incident af te handelen.

5.6. Meldingen die worden gedaan op grond van artikel 5.2 worden ogenblikkelijk gericht aan Verwerkingsverantwoordelijke of, indien relevant, aan een door Verwerkingsverantwoordelijke tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte Medewerkers van Verwerkingsverantwoordelijke. Indien Verwerkingsverantwoordelijke een Functionaris voor de Gegevensbescherming (FG) heeft aangesteld, worden de meldingen gericht aan deze FG.

5.7. Het is Verwerker niet toegestaan informatie te verstrekken over Incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is of Partijen anderszins zijn overeengekomen.

5.8. Indien en voor zover Partijen zijn overeengekomen dat Verwerker in relatie tot een Incident rechtstreeks contact onderhoudt met autoriteiten of andere derde partijen, dan houdt de Verwerker de Verwerkingsverantwoordelijke daarvan voortdurend op te hoogte.

Artikel 6. Medewerkingsverplichtingen

6.1. De AVG en overige (privacy)wetgeving kent aan de Betrokkene bepaalde rechten toe. Verwerker zal zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke bij de nakoming van de op Verwerkingsverantwoordelijke rustende verplichtingen voortvloeiend uit deze rechten.

6.2. Een door Verwerker ontvangen klacht of een verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zonder uitstel doorgestuurd naar Verwerkingsverantwoordelijke.

6.3. Op het eerste daartoe strekkende schriftelijke verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van Persoonsgegevens.

6.4. Verwerker zal voorts op eerste schriftelijke verzoek van Verwerkingsverantwoordelijke alle noodzakelijke en redelijke bijstand verlenen bij de nakoming van de op grond van de toepasselijke privacywetgeving op Verwerkingsverantwoordelijke rustende wettelijke verplichtingen (zoals het uitvoeren van een privacy impact assessment).

Artikel 7. Inschakeling subverwerkers

7.1. Verwerkingsverantwoordelijke erkent en stemt er mee in dat Verwerker subverwerkers mag inzetten voor het verwerken van Persoonsgegevens. Verwerker stelt een lijst op met de belangrijkste subverwerkers en stelt Verwerkingsverantwoordelijke in staat kennis te nemen van eventuele nieuwe Subverwerkers. Verwerkingsverantwoordelijke kan binnen vijf (5) werkdagen na ontvangst van een bericht over een nieuwe Subverwerker bezwaar maken tegen het door Philips inschakelen van deze Subverwerker door objectieve gronden van bezwaar kenbaar te maken die verband houden met de mogelijkheid van de Subverwerker om de Persoonsgegevens te beschermen en Toepasselijk Recht na te leven. In dat geval zullen Partijen in goed vertrouwen samenwerken om een oplossing voor de bezwaren van verwerkingsverantwoordelijke te vinden, waaronder begrepen maar niet beperkt tot het beoordelen van aanvullende informatie waaruit de geschiktheid van de subverwerker zou moeten blijken of het uitvoeren van de Overeenkomst(en) en de Verwerkersovereenkomst zonder inschakeling van de betreffende subverwerker.

7.2. Verwerker zal aan de door hem ingeschakelde subverwerker dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst, de Philips Binding

Corporate Rules en de wet voortvloeien en ziet toe op de naleving daarvan door de derde. De betreffende afspraken met de subverwerker zal Verwerker schriftelijk vastleggen in een overeenkomst.

7.3. Niettegenstaande de toestemming van Verwerkingsverantwoordelijke voor het inschakelen van een Subverwerker die in opdracht van de Verwerker (gedeeltelijk) gegevens verwerkt, blijft Verwerker volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een Subverwerker. De toestemming van Verwerkingsverantwoordelijke voor het uitbesteden van werkzaamheden aan een subverwerker laat onverlet dat voor het inschakelen van subverwerkers in een land buiten de EER voorafgaande toestemming is vereist van Verwerkingsverantwoordelijke, niettegenstaande het bepaalde in artikel 3.7 van (dit addendum bij) deze Verwerkingsovereenkomst.

Artikel 8. Aansprakelijkheid

8.1. Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen.

8.2. De totale aansprakelijkheid van Verwerker voor alle aanspraken voortvloeiend uit een schending van Verwerkers verplichtingen op grond van deze Verwerkersovereenkomst, is beperkt tot de directe schade van Verwerkingsverantwoordelijke met een maximum van in totaal EUR 350.000,-. Verwerker is niet aansprakelijk voor indirecte en gevolgschade, waaronder – doch niet uitsluitend – gederfde winst of omzet, verlies van gebruik, verlies van goodwill, extra uren van werknemers of verlies van verwachte besparingen.

8.3. Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt de Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit een toerekenbare tekortkoming door Verwerker en/of diens onderaannemers/Subverwerkers in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerker en/of diens onderaannemers/Subverwerkers van de van toepassing zijnde wetgeving op het gebied van verwerking van Persoonsgegevens, voor zover dit plaatsvindt binnen de directe invloedssfeer van Verwerker. Verwerkingsverantwoordelijke vrijwaart Verwerker en stelt de Verwerker schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit een toerekenbare tekortkoming door Verwerkingsverantwoordelijke in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerkingsverantwoordelijke van de van toepassing zijnde wetgeving op het gebied van verwerking van Persoonsgegevens, voor zover dit plaatsvindt binnen de directe invloedssfeer van Verwerkingsverantwoordelijke. Op deze vrijwaring is de beperking van artikel 8.2 van overeenkomstige toepassing.

8.4. Voor zover Partijen hoofdelijk aansprakelijk zijn jegens derden, waaronder begrepen de betrokkene, of gezamenlijk een boete opgelegd krijgen door de Autoriteit Persoonsgegevens, zijn zij jegens elkaar, ieder voor het gedeelte van de schuld dat hem in hun onderlinge verhouding aangaat, verplicht overeenkomstig het bepaalde in Boek 6, Titel 1, Afdeling 2 van het Burgerlijk Wetboek in de schuld en kosten bij te dragen, tenzij de AVG anders bepaalt in welk geval de AVG voorgaat.

8.5. Voor zover in de Overeenkomst geen beperking van aansprakelijkheid voor Verwerkingsverantwoordelijke is opgenomen, geldt de in lid 2 opgenomen beperking voor Verwerker eveneens voor de Verwerkingsverantwoordelijke.

8.6. Iedere beperking van aansprakelijkheid komt voorts voor de betreffende Partij te vervallen in geval van opzet of grove schuld aan de zijde van de betreffende Partij.

8.7. Partijen dragen zorg voor afdoende dekking van de aansprakelijkheid.

Artikel 9. Kosten

9.1. De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Overeenkomst, worden geacht besloten te liggen in de op grond van de Overeenkomst reeds verschuldigde vergoedingen.

9.2. Enige ondersteuning of enige andere aanvullende dienstverlening die Verwerker op grond van deze Verwerkersovereenkomst dient te verlenen, of die wordt verzocht door Verwerkingsverantwoordelijke, inclusief alle verzoeken tot aanvullende informatie, zullen in rekening worden gebracht bij Verwerkingsverantwoordelijke overeenkomstig nader tussen Partijen overeen te komen tarieven.

9.3. De voorgaande bepaling is niet van toepassing indien de werkzaamheden verband houden met een tekortkoming van Verwerker onder deze Verwerkersovereenkomst. De werkzaamheden zullen in dat geval kosteloos worden verricht (onverminderd het recht van Verwerkingsverantwoordelijke de daadwerkelijk geleden schade op Verwerker te verhalen).

Artikel 10. Duur en beëindiging

10.1. Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de in Bijlage 1 genoemde Overeenkomst(en), inclusief eventuele verlengingen daarvan.

10.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onlosmakelijk deel uit van de Overeenkomst(en). Beëindiging van de Overeenkomst(en), op welke grond dan ook (opzegging/ontbinding), heeft tot gevolg dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij Partijen in voorkomend geval anders overeenkomen.

10.3. Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze bepalingen behoren bijvoorbeeld die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid, geschillenbeslechting en toepasselijk recht.

10.4. Ieder der Partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Overeenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Overeenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:

a.) de andere Partij wordt ontbonden of anderszins ophoudt te bestaan;

b.) de andere Partij aantoonbaar [ernstig] tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;

c.) een Partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.

10.5. Gelet op de grote afhankelijkheid van Verwerkingsverantwoordelijke van Verwerker alsmede het continuïteitsrisico bij incidenten en calamiteiten (zoals faillissement), verklaart Verwerker zich reeds nu voor alsdan bereid om indien er sprake is van incidenten en/of calamiteiten, op

eerste verzoek van Verwerkingsverantwoordelijke in overleg te treden over aanvullende afspraken.

10.6. Vervalt.

10.7. Verwerkingsverantwoordelijke is gerechtigd deze Verwerkersovereenkomst per direct te ontbinden als Verwerker aan Verwerkingsverantwoordelijke schriftelijk te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet aan de verwerking van Persoonsgegevens worden gesteld.

10.8. Vervalt.

10.9. Het is Verwerker niet toegestaan om zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke deze Verwerkersovereenkomst en de rechten en plichten die samenhangen met deze Verwerkersovereenkomst over te dragen aan een derde partij.

Artikel 11. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

11.1. Verwerker bewaart de Persoonsgegevens niet langer dan de tussen Partijen gemaakte afspraak over bewaartermijnen zoals vastgelegd in Bijlage 1. Verwerkingsverantwoordelijke bepaalt of en zo ja hoe lang gegevens bewaard moeten blijven.

11.2. Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker tegen redelijke kosten naar keuze van Verwerkingsverantwoordelijke de Persoonsgegevens (doen) vernietigen of teruggeven aan Verwerkingsverantwoordelijke, behoudens voor zover Verwerker bevoegd en/of gehouden is Persoonsgegevens te bewaren op grond van de wet. Op verzoek van Verwerkingsverantwoordelijke zal Verwerker de vernietiging schriftelijk aan Verwerkingsverantwoordelijke bevestigen. Eventuele teruggave van Persoonsgegevens zal in een gangbaar gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verwerkingsverantwoordelijke hiervan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de Persoonsgegevens vertrouwelijk zal behandelen en niet verder zal verwerken (met uitzondering van het bewaren).

Artikel 12. Intellectuele eigendomsrechten

12.1. Voor zover de (verzameling van) Persoonsgegevens wordt beschermd door enig intellectueel eigendomsrecht, verleent Verwerkingsverantwoordelijke toestemming aan Verwerker de Persoonsgegevens te gebruiken in het kader van de uitvoering van deze Verwerkersovereenkomst.

Artikel 13. Slotbepalingen

13.1. De overwegingen maken onderdeel uit van deze Verwerkersovereenkomst.

13.2. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

13.3. In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen Partijen in onderling overleg.

13.4. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

13.5. Partijen zullen zich inspannen conflicten in onderling overleg op te lossen. Hierbij is inbegrepen de mogelijkheid het geschil te beëindigen door een in onderling overleg vast te stellen mediation of arbitrage.

13.6. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Overeenkomst aangewezen rechtbank of arbiter(s).

Bijlage 1: Overeenkomsten, omschrijving Persoonsgegevens, aard verwerkingen, etc.

Deze Verwerkersovereenkomst is van toepassing op het gebruik van het Portaal in overeenstemming met de Gebruikersvoorwaarden, waarvan deze Verwerkersovereenkomst deel uit maakt (de "Overeenkomst").

Korte omschrijving diensten	Aard van de verwerking	Soort Persoonsgegevens	Categorieën van betrokkenen	Doeleinden van de verwerking
Het leveren, hosten en onderhouden een online portaal, aangeboden als cloudoplossing, voor het uitwisselen van patiëntgegevens tussen ziekenhuizen.	Verwerking van patiëntgegevens, loggegevens en metadata.	Patiëntgegevens in de ruimste zin van het woord, waaronder, NAW-gegevens, medische gegevens (waaronder radiologische beelden, laboratoriumuitslagen en verslagen) en de inloggegevens van gebruikers van het portaal.	Patiënten en gebruikers van het Portaal.	Uitwisselen van patiëntgegevens tussen ziekenhuizen.

Goedgekeurde subverwerkers

1) Intermax, gevestigd in Nederland, ten behoeve van de "managed hosting services";
2) TOPdesk, gevestigd in Nederland, ten behoeve van de registratie van support tickets;
3) Harbers ICT, gevestigd in Nederland, ten behoeve van de tweede en derdelijns ondersteuning van de IT afdeling;
4) Webr, gevestigd in Nederland, ten behoeve van de tweede en derdelijns ondersteuning van de IT afdeling;
5) Koninklijke Philips N.V. en aan haar gelieerde vennootschappen, ten behoeve van de ondersteuning van Forcare Holding B.V. bij de uitvoering van haar verplichtingen onder de Privacy Voorwaarden en de Gebruikersvoorwaarden.

Bijlage 2 – Beschrijving van beveiligingsmaatregelen

Philips Product & Services beveiligingsbeleidskader

Producten en aan een product gerelateerde services, zoals Connected / Remote Service Infrastructuur, hosting oplossingen en platformen, customer services applicaties zijn vitale bedrijfsmiddelen, die essentieel zijn voor Philips als bedrijf en voor klanten van Philips. Het beveiligingsbeleid van Philips Product & Services Security bevat een reeks gedefinieerde beleidsregels, standaarden, richtlijnen, procedures en processen die zorgen voor de Security by Design en operational excellence doelstellingen. Elk Philips product en elke Philips service integreert de juiste maatregelen die van toepassing zijn op het bedoelde gebruik en beheer van het product of de service.

Gegevens- en systeembeveiliging

In overeenstemming met de interne Philips-informatiebeveiligingsnormen zijn passende technische en organisatorische beveiligingsmaatregelen geïmplementeerd, die een beveiligingsniveau waarborgen dat is afgestemd op de beveiligingsrisico's van het product of service, hierbij rekening houdend met de implementatiekosten, de aard, de omvang en context van gegevensverwerking. Hieronder volgt een overzicht van de beleidsmaatregelen, procedures en processen die de technische, fysieke en organisatorische maatregelen bevatten die Philips toepast om de gegevens van haar zakelijke klanten die persoonsgegevens (ZKP-gegevens) bevatten te beschermen tegen vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

Beveiliging van personeel

Alle medewerkers van Philips die toegang hebben tot ZKP-gegevens, zijn getraind in rollen en verantwoordelijkheden die van toepassing zijn in de mate die nodig is om hun functie uit te voeren en de verwerking volgens de Philips General Business Principals. Philips legt een verplichting tot vertrouwelijkheid op aan Philips-medewerkers die toegang hebben tot ZKP-gegevens.

Risicoanalyse en -management

Philips onderhoudt een veelomvattende risicomanagement strategie met een holistisch proces voor risicoanalyse om beveiligingsrisico's te voorkomen, te beperken en/of op te heffen en periodiek het beveiligingsniveau te controleren gedurende de gehele levenscyclus van het product of de service. Philips heeft gecategoriseerde beveiligingseisen opgesteld (bijvoorbeeld toegangscontroles, codering, systeemverharding, patches, malwarebescherming, kwetsbaarheidsbeheer, codebeoordelingen, trainingen voor informatiebeveiliging en monitoring van informatiebeveiliging) om adequate beperking en bescherming van systeem- en informatiemiddelen te waarborgen.

Toegangsbeveiliging

Een op rollen gebaseerde toegangscontrole zijn ingericht om de toegang tot systemen en gegevens te beperken tot door management bevoegde personen en voor uitsluitend geldige zakelijke doeleinden. Medewerkers van Philips en derden die ZKP-gegevens verwerken zijn, per gedefinieerde rol, getraind en verantwoordelijk voor de bescherming van die informatie en de daaraan gerelateerde bedrijfsmiddelen.

Bedrijfscontinuïteit

De eisen die gesteld worden aan de beveiliging van producten en diensten garanderen de doorlopende integriteit, beschikbaarheid en voldoende redundantie van verwerkingssystemen en -services om ervoor te zorgen dat Philips-producten en -services over adequate back-up- en herstelprocedures beschikken in overeenstemming met de gedefinieerde herstelgaranties. Systemen kunnen hun activiteiten op een minimaal niveau voortzetten en de volledige functionaliteit herstellen in het geval van een grote verstoring van de activiteiten. Rampenplannen en procedures worden getest en geverifieerd.

Activiteitenregistratie

Philips' Security & Privacy beleidsregels vereisen een correcte registratie en monitoring voor het vastleggen van relevante acties en toegang tot systemen, gerelateerd aan informatiebeveiliging. Veiligheidscontrolefuncties, serviceniveaus en managementvereisten van alle netwerkdiensten moeten zijn geïdentificeerd en opgenomen in elk netwerkservicecontract, ongeacht of deze services intern worden geleverd of worden uitbesteed. Ook zijn formele procedures nodig om toegang tot systemen of applicaties te autoriseren en alle toegangsrechten en rechten voor gebruikers moeten periodiek worden beoordeeld.

Beveiligingsincidenten en melding van inbreuk

Alle werknemers, contractanten en externe gebruikers van informatiesystemen en services zijn verplicht om geconstateerde of vermoedelijke zwakke punten in de beveiliging van systemen of services, via het lijnmanagement, op te merken en te rapporteren aan Philips PSIRT (Product Security Incident Response Team) voor onderzoek en, indien van toepassing, verdere afhandeling. Product & Services Beveiligingsincidenten waarbij persoonlijke gegevens zijn betrokken of die mogelijk implicaties voor de privacy hebben, moeten ook worden gemeld aan de aangewezen Privacy Officer.

Philips zal de zakelijke klant op de hoogte brengen van een inbreuk op de gegevensbeveiliging zoals vereist door de wet of zo snel als redelijkerwijs mogelijk is, na ontdekking van een dergelijke inbreuk, tenzij een wetshandhavingsfunctionaris of toezichthoudende instantie bepaalt dat die kennisgeving een (strafrechtelijk) onderzoek zou verhinderen of schade zou toebrengen aan de nationale veiligheid of het vertrouwen in de industriesector. In dat geval wordt de kennisgeving vertraagd op verzoek van die rechtshandhavingsfunctionaris of toezichthoudende autoriteit. Philips zal onmiddellijk reageren op vragen van de zakelijke klant met betrekking tot een dergelijke inbreuk op de gegevensbeveiliging.

Fysieke beveiliging

Het beveiligingsbeleid van Philips Product & Services vereist dat Philips' management de gebieden identificeert die een specifiek niveau van fysieke beveiliging vereisen. Toegang tot die gebieden wordt alleen verleend aan geautoriseerde personen voor geautoriseerde doeleinden. Philips' beveiligde zones maken gebruik van verschillende fysieke veiligheidswaarborgen, waaronder bewaking van gesloten tv-schermen, gebruik van beveiligingsbadges (identiteitsgestuurde toegang) en beveiligingsmedewerkers bij in- en uitgangen. Bezoekers mogen alleen toegang krijgen waar ze zijn geautoriseerd en moeten te allen tijde worden gecontroleerd.

Naleving

Philips heeft een Product & Services Security Office dat regelmatig de geïmplementeerde beveiligingsmaatregelen en de implementatie van nieuwe beveiligingsvereisten controleert. Naleving

van het beveiligingsbeleid van Philips Product & Services wordt bereikt door jaarlijkse training, periodieke beoordelingen van lokale en organisatie brede beleidsregels en procedures, en audits.

Philips Remote Service Network

Philips Remote Services heeft beveiligingsmaatregelen geïmplementeerd die voldoen aan de eisen zoals gesteld door de internationale ISO 27001-norm ten behoeve van managementsystemen voor informatiebeveiliging en die jaarlijks worden getoetst door een onafhankelijke derde partij. Het ISO 27001 certificaat is op aanvraag beschikbaar. Voorts voldoen de beveiligingsmaatregelen aan NEN7510. Wederom is het certificaat op aanvraag beschikbaar.