Gedragscode voor leveranciers:

Informatieveiligheid & gegevensbescherming

Voor alle bijkomende vragen i.v.m. dit document kan u terecht bij de DPO of de aankoopdienst.

Inhoudsopgave

Doel

Het ziekenhuis heeft de wettelijke verplichting om een informatieveiligheidsbeleid en –plan op te stellen en uit te voeren met als doel:

1. De persoonlijke levenssfeer en informatieveiligheid van de patiënten, individuele gebruikers, artsen en medewerkers te beschermen;
2. De rechten en de plichten voor externe medewerkers, leveranciers en dienstverleners en hun onderaannemers van het Jan Yperman ziekenhuis te bepalen;
3. De veiligheid, de betrouwbaarheid en dienstverlening te waarborgen van de systemen en netwerken van het Jan Yperman Ziekenhuis.

Met deze gedragscode wenst het Jan Yperman Ziekenhuis haar verwachten ten aanzien van haar (huidige/ toekomstige/ mogelijke) leveranciers te communiceren.

Aankoopproces: verwachtingen ten aanzien van de leverancier

Documenten inzake vertrouwelijkheid en gegevensbescherming

MDS2-formulier: Manufacturer Disclosure statement for medical Device security

Indien de mogelijke aankoop betrekking heeft op medische toestellen, verwacht het Jan Yperman Ziekenhuis dat de leverancier het MDS2-formulier overmaakt.
Het MDS2 is een middel om tijdens het inkoopproces informatie te verkrijgen over de security en privacy kenmerken van een medisch apparaat/ systeem en om verder te worden gebruikt in het risicomanagement van bijvoorbeeld een zorginstelling.

Het MDS2 wordt door de leverancier bezorgd aan de DPO en IT-dienst (security@yperman.net) voor de verdere beoordeling van de offerte.

Verwerkersovereenkomst

Indien er persoonsgegevens verwerkt worden, is de Algemene Verordening Gegevensbescherming (AVG/ GDPR) van toepassing. Onder de verwerking verstaat het ziekenhuis dat een leverancier toegang heeft tot persoonsgegevens d.m.v.:

1. **Persoonsgegevens raadplegen**: diensten van de leverancier waarbij de persoonsgegevens van het Ziekenhuis bekeken kunnen worden door medewerkers of onderaannemers van de leverancier,
2. **Persoonsgegevens opslag**: diensten van de leverancier waarbij de persoonsgegevens van het Ziekenhuis opgeslagen worden in een door de leverancier geleverd opslagsysteem;
3. **Persoonsgegevens doorzenden**: diensten van de leverancier waarbij persoonsgegevens van het Ziekenhuis verzonden worden van, naar of tussen applicaties op een door de leverancier beheerd platform;
4. **Persoonsgegevens bijwerken of wijzigen**: diensten van de leverancier waarbij persoonsgegevens van het Ziekenhuis aangepast kunnen worden zowel op manuele, als op geautomatiseerde wijze zoals bij een geautomatiseerde job flow die ondersteund wordt door een job scheduling system.

5. **Software testen**: diensten van de leverancier waarbij databanken van het Ziekenhuis die persoonsgegevens bevatten (persoonsgegevens die niet geanonimiseerd zijn), worden gebruikt buiten de productie omgeving (in test, acceptatie,…) als onderdeel van het testproces van de Ziekenhuis software applicatie.
6. **Remote support**: gedurende het opsporen en verhelpen van software- of hardware problemen kan raadpleging van persoonsgegevens mogelijk zijn. Consultatie van deze gegevens kan gebeuren vanop afstand waarbij de vastgelegde instructies door het Ziekenhuis nageleefd worden qua autorisatie en aanloggen. Er gebeuren geen andere bewerkingen dan deze hierboven beschreven. Gegevens worden niet systematisch opgeslagen, verzameld, gewijzigd of gewist.

Het Jan Yperman ziekenhuis verwacht dat de leverancier de modelverwerkersovereenkomst (gebaseerd op het model Zorgnet-Icuro) ondertekent, die integraal als onderdeel van het aanbod in zijn offerte zal worden beschouwd.
Enig voorbehoud betreffende deze overeenkomst en de erin opgenomen garanties zal leiden tot de nietigheid van de offerte. In annex 5 kunnen geen afwijkingen in negatieve zin voor het Jan Yperman ziekenhuis toegestaan worden.
De verwerkersovereenkomst is in PDF terug te vinden op de website van het ziekenhuis (zie Leveranciers). Een Word-versie kan aangevraagd worden bij de DPO.
De verwerkersovereenkomst wordt door de leverancier ondertekend en wordt terug bezorgd aan de DPO (dpo@yperman.net) voor de verdere beoordeling van de offerte.

<u>Leveranciersbeoordeling informatieveiligheid, ISO 27001 en CyFun</u>

Het Jan Yperman Ziekenhuis verwacht dat de leverancier die persoonsgegevens verwerken en die bedrijfskritische applicaties (incl. informatie- en netwerksystemen) aanleveren, bij voorkeur over een ISO 27001 certificaat beschikt of aantoont dat het volgens de geest van de ISO 27001 standaarden te werken. Het Ziekenhuis accepteert ook CyFun certificatie.

Het ziekenhuis kan aan elke leverancier vragen om een ‘vragenlijst leveranciersbeoordeling informatieveiligheid’ in te vullen, vóór het afsluiten van de overeenkomst.
De leverancier bezorgt daarvan het resultaat onverwijld aan de DPO en de IT afdeling van het ziekenhuis (security@yperman.net).

Aanvaarding van de opdracht

Door aanvaarding van de opdracht en/of door verdere samenwerking:

- Gaat de leverancier akkoord met de voorwaarden zoals vastgesteld in deze gedragscode. De verkoopvoorwaarden van de leverancier zijn, ongeacht de benaming die eraan wordt gegeven door de leverancier, niet van toepassing indien ze strijdig zijn met de bepalingen van deze gedragscode;
- verklaart en bevestigt de leverancier dat alle gegevens naar waarheid zijn ingevuld en/of doorgegeven.

Dienstverlening door de leverancier

Bij plaatsbezoek in het ziekenhuis

Professionele bezoekers in niet publieke zones

Leveranciers die het ziekenhuis binnenkomen in het kader van een dienstverlening en die zich – **zonder begeleiding** van een medewerker van het Jan Yperman Ziekenhuis –in de **niet-publieke zones** moeten begeven, moeten zich steeds aan- en afmelden aan de voorziene kiosk of badgelezer. Zo weten we op elk ogenblik wie er in ons ziekenhuis aanwezig is.

Leveranciers die werken komen uitvoeren **in opdracht van de (bio-)technische dienst** hebben twee opties:

1. Voor leveranciers die regelmatig komen, zijn er één of meerdere badges verkrijgbaar op naam van de leverancier (25 EUR waarborg per badge)
2. Voor leveranciers die maar sporadisch komen, kunnen deze bij aankomst een badge afhalen op het secretariaat (8u – 16u30) van de technische dienst of voor het medische luik op de biotechnische dienst.

Vanaf 01 december 2022 is dan ook iedereen verplicht “IN” te badgen (bij aankomst) en “UIT” te badgen (bij vertrek). Dit kan tijdens de kantooruren gebeuren aan de deur van secretariaat Technische Dienst. Buiten de kantooruren kan dit links van de buitendeur Technische Dienst.
Bij het niet badgen, veronderstellen we geen aanwezigheid en bijgevolg betalen we geen factuur voor deze gepresteerde uren.

Secretariaat Technische dienst

Buitendeur Technische dienst

Overige leveranciers (ondersteuning preventie op het werk, auditoren, consultants IT, etc.) kunnen zich aanmelden aan de kiosk aan de receptie. Zij ontvangen op voorhand een QR-code om te kunnen inloggen. Indien de bezoeker geen QR-code heeft, moet hij zich aanmelden aan de receptie, die dan alsnog een vooraanmelding kan maken en de badge kan afdrukken. Bij het uitbadgen ontvangt de bezoeker via de kiosk een gratis parkeerticket.

Kiosk aan de receptie

Een leverancier moet steeds zijn ticket of badge op een zichtbare plaats dragen in het Jan Yperman Ziekenhuis.

<u>Technische adviseurs in het operatiekwartier</u>
De toegang van technische adviseurs die namens een leverancier aanwezig moet zijn in het operatiekwartier, wordt geregeld via het “Reglement inwendige orde operatiekwartier”:

De medewerker meldt zich bij iedere komst aan via de voorziene kiosk aan de receptie. Indien de medewerker geen QR-code heeft, moet hij zich aanmelden aan de receptie, die dan alsnog een vooraanmelding kan maken en de badge kan afdrukken. Bij het uitbadgen ontvangt de medewerker via de kiosk een gratis parkeerticket. Daarna meldt de medewerker zich aan bij de hoofdverpleegkundige/ planner of zijn vervanger van het operatiekwartier.

Bij gebruik van ziekenhuisapparatuur of netwerk (algemeen)
De computersystemen en andere ICT-apparatuur die toebehoren aan het Jan Yperman ziekenhuis mogen enkel gebruikt worden binnen de grenzen van de toevertrouwde professionele opdracht.
Indien praktische omstandigheden een uitzondering vereisen kunnen die enkel toegestaan worden na uitdrukkelijk overleg met en goedkeuring van het de IT-manager.

De leverancier en de medewerkers onder zijn verantwoordelijkheid verbinden zich ertoe de onderstaande richtlijnen te volgen:

- op IT-apparatuur van het ziekenhuis:
    - o enkel software te gebruiken die door het ziekenhuis wordt verstrekt en dit overeenkomstig de specifieke richtlijnen en geen andere software te installeren en/of te gebruiken;
    - o de ingestelde veiligheidsmaatregelen (bv. de virusscanner) niet uit te schakelen;
- alle bestanden verkregen via een extern netwerk of verschaft op draagbare media nodig voor de opdracht, te controleren om na te gaan of deze virusvrij zijn alvorens deze te gebruiken tijdens de opdracht;
- geen gegevens van het ziekenhuis en zijn activiteiten die er mee gepaard gaan op dragers te kopiëren of aan derden mee te delen;
- toegang tot beveiligde IT-ruimtes en afgeschermde netwerkapparatuur enkel onder supervisie van de dienst IT te laten plaatsvinden;

- geen foto's of filmpjes nemen en/of publiceren waarop patiënten of ziekenhuismedewerkers herkenbaar zijn.

Het is niet toegelaten apparatuur aan het ziekenhuisnetwerk te koppelen of wijzigingen aan te brengen aan de bestaande infrastructuur zonder de schriftelijke toestemming van de dienst IT.
Dit geldt zowel voor het bekabeld als draadloos netwerk en voor elke apparatuur (al dan niet eigendom van het ziekenhuis). De leverancier dient de nodige toegangsrechten aan de IT-manager van het ziekenhuis te verstrekken betreffende de systemen die niet vallen onder het IT-beheer van het ziekenhuis.

Shares op het netwerk mogen enkel door of in opdracht van de medewerkers van de dienst IT van het ziekenhuis aangemaakt of gewijzigd worden. Extern gebruik van het interne netwerk van het ziekenhuis is alleen toegestaan aan de daartoe geautoriseerde personen en moet via een goedgekeurde en geregistreerde firewall lopen.

Systemen die gebruikt worden voor externe aansluiting aan het ziekenhuisnetwerk dienen voorzien te zijn van up-to-date beschermingstools conform de ISO-normering. Daarnaast dient de externe gebruiker erop toe te zien dat de systeemsoftware op zijn systeem wordt onderhouden op een actueel patchniveau. Externe connecties worden na een door het ziekenhuis vast te stellen periode van inactiviteit automatisch beëindigd. De externe gebruiker wordt geacht zich te onthouden van de toepassing van periodieke processen om de verbinding kunstmatig in stand te houden.

Bij gebruik van het EPD

In uitzonderlijke situaties is het noodzakelijk dat medewerkers van een leverancier toegang verkrijgen tot het Elektronisch Patiëntendossier (EPD).
Deze toegangen worden toegekend na een gunstig advies van de "Werkgroep digitaal toegangsbeheer- en beleid".
De leverancier bezorgt aan de DPO (dpo@yperman.net) een lijst van de betrokken medewerkers met daarbij volgende gegevens (noodzakelijk voor de rechtentoekenning): naam, voornaam, functie, einddatum indien contract van bepaalde duur, geboortedatum, geboorteplaats en rijksregisternummer.
Het Jan Yperman Ziekenhuis verwacht dat elke medewerker met toegang tot het EPD, de confidentialiteitsverklaring in bijlage 1A ondertekent.

Bij gebruik van internet

Het gebruik van internet vanuit de server is mogelijk indien de IT dienst ruim op voorhand geïnformeerd wordt over de nodige IP 's en poorten voor het tot stand brengen van de connectie.
Deze connecties worden gemonitord en eventueel onderbroken bij detectie van gevaren naar het ziekenhuis. Daarnaast dient de leverancier de IT dienst eveneens te informeren indien grote hoeveelheden data getransfereerd worden, zo niet kan de verbinding plots verbroken worden.

Toegang vanop afstand (VPN)

- Er wordt enkel een verbinding opgezet op vraag van of na overleg met de IT-Dienst. Elke andere verbinding wordt beschouwd als een elektronische inbraak en kan strafrechtelijk vervolgd worden.
- De IT Dienst behoudt zich het recht voor om de VPN-connectie en/of gebruikers te deactiveren wanneer men zich niet aan bovenstaande afspraak houdt.
- De VPN-regels worden standaard enkel geactiveerd na vraag van de leverancier en opnieuw gedeactiveerd na een vastgelegde tijd of na signaal van de leverancier dat

deze zijn taak beëindigd heeft. Hierbij heeft de firma steeds een duidelijke omschrijving van de reden waarom er toegang nodig is. Daarnaast houdt de firma ook een automatische en beveiligde logging bij omtrent het gebruik van deze toegang, zodat men steeds in staat is om een overzicht te geven van wie wanneer en waarom toegang had tot onze systemen.

- De leverancier doet het nodige om de remote toegang voldoende te beveiligingen tegen onbevoegden.
- Alle gegevens die tijdens de toegang of via de eindgebruikers vernomen worden, dienen strikt vertrouwelijk behandeld te worden en mogen voor geen enkel ander doeleinde gebruikt worden dan het bieden van support.
- Het is niet toegestaan om zonder onze schriftelijke toestemming een kopie te nemen van gegevens die eigendom zijn van het ziekenhuis.
- Wanneer men een kopie bezit van gegevens die eigendom zijn van het ziekenhuis, dan moeten deze altijd strikt vertrouwelijk behandeld worden en mag deze enkel gebruikt worden voor het zoeken naar de oplossing van een gemeld probleem.
- Een kopie van gegevens die eigendom zijn van het ziekenhuis mag enkel bestaan gedurende de tijd die nodig is voor de oplossing van het probleem. Na oplossing van dit probleem moet deze kopie en alle andere mogelijke exemplaren (back-ups e.d.) definitief vernietigd worden. Een gewone delete volstaat niet. Fysische vernietiging van het medium (CD-R en andere externe mediadragers) of gecertifieerde vernietiging door software op harde schijf moet altijd gebeuren.

Toezicht en controle

Principes

Externe medewerkers, leveranciers, dienstverleners en hun onderaannemers aanvaarden dat het ziekenhuis controles uitvoert om eventuele onregelmatigheden m.b.t. het gebruik van haar apparatuur en systemen op te sporen en om de naleving van de verplichtingen opgesomd in deze gedragscode te controleren en dit binnen de wettelijke beperkingen met betrekking tot de volgende situaties:

- de preventie van ongeoorloofde feiten of van feiten die indruisen tegen de goede zeden of die de waardigheid van andere personen kunnen aantasten;
- de bescherming van de belangen van de instelling, onder meer tegen informatielekken of een verkeerd gebruik van de informatie;
- de veiligheid en/of de goede technische werking van de functionerende informaticasystemen van de instelling.

Sancties

Voor externe medewerkers, leveranciers, dienstverleners en hun onderaannemers zal de juridische werkgever op de hoogte gesteld worden van de inbreuk en de eventuele tijdelijke of definitieve herroeping van de autorisatie tot gevolg hebben.
Daarnaast kan een inbreuk aanleiding geven tot een verbod van toegang tot de gebouwen en toepassingen van het ziekenhuis.
Indien de externe medewerkers, leveranciers, dienstverleners en hun onderaannemers hun verplichtingen, voortvloeiend uit deze gedragscode niet, niet tijdig of niet naar behoren nakomen blijven zij van rechtswege in gebreke.

Bijlagen

Confidentialiteitsverklaring EPD (bijlage 1A)

VZW Jan Yperman Ziekenhuis beschikt over een elektronisch patiëntendossier (EPD) voor de verwerking van persoonsgegevens van zijn patiënten. Het ziekenhuis gebruikt hiervoor het Klinisch Werkstation (KWS) van Nexuzhealth.

De extern samenwerkende partij kan tijdelijk en voorwaardelijk, toegang tot dit EPD krijgen.

Ik (*) ondergetekende,
……..……(naam), geboren op ……..(datum) te ……(geboorteplaats) met rijksregisternummer …… en werknemer in het ……(werkgever), verklaart hierbij akkoord te zijn met onderstaande richtlijnen

- Ondergetekende respecteert de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de algemene verordening gegevensbescherming (AVG of GDPR), de wet van 22 augustus 2002 betreffende de rechten van de patiënt en de wet van 22 april 2019 inzake de kwaliteitsvolle praktijkvoering in de gezondheidszorg.
- Ondergetekende heeft kennis van de 'gedragscode KWS' en leeft deze strikt na.
- Ondergetekende verschaft zich enkel toegang tot de persoonsgegevens en vertrouwelijke (bedrijfs)informatie die noodzakelijk zijn voor zijn/haar opdracht.
- Ondergetekende is discreet en deelt persoonsgegevens en vertrouwelijke (bedrijfs)informatie enkel met de personen bevoegd om er kennis van te nemen. Ondergetekende staat er voor in steeds zorgvuldig af te wegen of deze personen recht hebben op deze informatie en of dit in het belang is van de dienstverlening of het functioneren van het Jan Yperman Ziekenhuis.
- Indien van toepassing voor zijn/haar functie, neemt ondergetekende het beroepsgeheim in acht.
- Ondergetekende gebruikt de persoonsgegevens en vertrouwelijke (bedrijfs)informatie nooit in het nadeel van het Jan Yperman Ziekenhuis of betrokkene, voor persoonlijke doeleinden of voor andere professionele activiteiten die buiten het doel van de toegang vallen.
- Ondergetekende geeft toegangscodes- en middelen, wachtwoorden, enz. die hem/haar toegang verschaffen tot persoonsgegevens en vertrouwelijke (bedrijfs)informatie niet door.
- Ondergetekende beperkt het transport van persoonsgegevens en vertrouwelijke (bedrijfs)informatie tot een absoluut minimum en doet hierbij al het mogelijke om te voorkomen dat gegevens worden vrijgegeven aan onbevoegden, gestolen of verloren geraken.
- Ondergetekende meldt onmiddellijk elke inbreuk in verband met persoonsgegevens (datalek), hoe gering ook, via dpo@yperman.net.
- Ondergetekende zal, zo nodig, medewerking verlenen bij het uitvoeren van de verplichtingen van de verwerkingsverantwoordelijke.

Vastgestelde overtredingen (bv. op basis van de logging) of klachten van patiënten kunnen onmiddellijk leiden tot het afsluiten van de toegang en/of het betalen van een schadevergoeding.

Bijlage

- **Bijlage 1. Gedragscode KWS**

Naam:
Datum:

_____
Handtekening

(*) De persoonsgegevens zoals naam, geboortedatum, geboorteplaats en rijksregisternummer zijn noodzakelijk voor het aanmaken van een account in het EPD. Voor meer informatie over de verwerking van persoonsgegevens kan u contact opnemen met de DPO via dpo@yperman.net.