

Privacysset

Kenmerk: 20.002

In de Privacysset vind je vijf werkvormen. In dit document hebben we wat extra informatie opgenomen.

Bij een aantal vragen of opdrachten is het niet mogelijk een eenduidig antwoord te geven. Dit kan namelijk afhangen van het eigen beleid in jullie zorginstelling. Sommige instellingen zijn strikter in de leer dan anderen of er zijn gewoon andere afspraken. Dat wil niet zeggen dat dat fout is, het is een kwestie van interpretatie.

Wil je meer informatie, heb je vragen of wil je je ervaringen met ons delen? Neem dan contact op met PrivacyLab via support@privacylabnederland.nl of 085-1302372

Veel plezier!

Dossier gluren

Hierbij de antwoorden/overwegingen bij de verschillende situaties. In een aantal situaties is sprake van inzage die niet is toegestaan. Ook al heb je een beroepsgeheim dan nog is inzage in gegevens waartoe je niet gerechtigd bent (je hebt geen behandelrelatie en je bent niet anderszins geautoriseerd) niet toegestaan. Dergelijke onterechte inzage kan voor jou zelfs arbeidsrechtelijke consequenties hebben.

Wanneer je opmerkt dat anderen dit doen dan zou je het gesprek met hen kunnen aangaan. Als je dat niet aandurft is een melding aan de privacy-officer of FG van je organisatie op zijn plaats.

Je kunt met elkaar spreken over de inrichting van de functiescheiding en de op basis daarvan ingerichte autorisatiematrix: zijn er collega's die consequent te veel of te weinig inzage hebben. Zijn er bijvoorbeeld functies gewijzigd en zijn de autorisaties niet mee gewijzigd?





Dossier gluren		
1.	Een cliënt van je is verhuisd naar een andere afdeling. Hoe is het nu met hem? Eens even opzoeken in het elektronisch cliëntendossier.	Niet oké. Je hebt geen behandelrelatie meer. Je kunt natuurlijk altijd zelf even langsgaan bij die persoon en persoonlijk informeren.
2.	De bewindvoerder van een cliënt vraagt inzage in het zorgdossier van deze cliënt.	Niet oké. Een bewindvoerder gaat alleen over financiën.
3.	De moeder van een bekende voetballer is bij jullie komen wonen. Toch interessant om te weten hoe het met haar is. Misschien staat er ook nog wel iets over de familieleden in het dossier?	Niet oké. Nieuwsgierigheid is soms begrijpelijk maar onder professioneel gedrag hoort dat je dit niet doet, ook al heb je een beroepsgeheim.
4.	Je weet dat een collega op een andere afdeling erg goed is in zorgplannen schrijven en dat wil jij ook graag leren. Om te kijken hoe ze dat doet open je een van de zorgplannen die zij geschreven heeft.	Dit kan zijn toegestaan, afhankelijk van het beleid in jullie zorginstelling. Vraag dit na bij je leidinggevende of jullie Functionaris voor Gegevensbescherming. Wie dat is? Dat hoor je op de website van je organisatie te kunnen vinden bij het onderwerp: privacy. Je kunt ook voorstellen om een of meer zorgplannen ter instructie te laten anonimiseren en die als voorbeeld te gebruiken. Misschien zijn er meer collega's die daarvan kunnen profiteren.



Dossier gluren		
5.	Je bent bestuurder van de zorginstelling en je bent verantwoordelijk voor alle cliënten. Dus je hebt toegang tot alle dossiers.	In de meeste instellingen heeft de bestuurder geen toegang tot zorgdossiers. Bij het vervullen van de taken is toegang tot (medische) gegevens van individuen niet noodzakelijk. Er bestaan echter ook (meestal kleinere) instellingen waar de bestuurder ook cliënten en hun familie te woord staat. Dan zou (gedeeltelijke) toegang tot dossiers nodig kunnen zijn. In de autorisatiematrix van het ECD is vastgelegd wie op welke onderdelen van het dossier van een cliënt toegang heeft. Zo'n matrix wordt meestal beheerd door applicatiebeheer of ICT.
6.	Je bent van de afdeling interne controle en je opent dossiers om te kijken of de doelen in het zorgplan op de juiste manier zijn beschreven.	Dit kan zijn toegestaan, afhankelijk van het beleid in jullie zorginstelling. Vraag dit na bij je leidinggevende of jullie Functionaris voor Gegevensbescherming. Wie dat is? Dat hoor je op de website van je organisatie te kunnen vinden bij het onderwerp: privacy. In de autorisatiematrix (zie ook bij 5) is vastgelegd tot welke delen van dossiers je toegang hebt. Controleer zelf of je toegang goed is ingesteld. Te weinig maar ook te veel rechten meld je bij je leidinggevende, de applicatiebeheerder of de Functionaris Gegevensbescherming.
7.	Je bent van de afdeling kwaliteit en je stelt een rapport op over het aantal vrijheidsbeperkende maatregelen. Daarvoor bestudeer je een aantal zorgdossiers.	Dit kan zijn toegestaan, afhankelijk van het beleid in jullie zorginstelling. Vraag dit na bij je leidinggevende of jullie Functionaris voor Gegevensbescherming. Wie dat is? Dat hoor je op de website van je organisatie te kunnen vinden bij het onderwerp: privacy. Zie ook de opmerking bij 6 over de autorisatiematrix.



Dossier gluren		
8.	Je was als verzorgende gisteren invalkracht op een andere afdeling en er was een incident met een bewoner. Hoe is dat afgelopen? Je zoekt het op in het elektronisch cliëntendossier.	Niet oké. Je hebt geen behandelrelatie meer. Via logbestanden wordt dit geregistreerd en dan kun je erop worden aangesproken.
9.	Je werkt op de administratie en opent een dossier om de indicatie aan te passen.	Bij werk op de zorgadministratie hoort toegang tot een beperkt gedeelte van het dossier. Als het goed is worden indicaties via Vecozo automatisch verwerkt in het systeem. Mocht er om uitzonderlijke redenen een aanpassing plaats moeten vinden dan hoort dat te gebeuren bij de zorgadministratie. Informeer hoe dit bij jullie geregeld is.
10.	Je zit in een intervisiegroepje en je collega zet een rapportage op het scherm om samen de situatie te bespreken.	Niet oké. Intervisie is een ander doel dan waarvoor je de gegevens verzameld hebt. Bij intervisie kun je situaties anoniem bespreken.
11.	Je hebt als manager straks een familiegesprek met een familie die een klacht heeft ingediend. Als voorbereiding neem je het dossier van de cliënt helemaal door.	Je moet als manager weten wat er speelt. De vraag is wel of je daar het hele dossier voor moet doornemen. Je kunt met elkaar spreken over de klachtenprocedure in jouw instelling. Je kunt de klachtenfunctionaris eens uitnodigen voor een teamoverleg om de afwikkeling van een klacht toe te lichten. Inzicht in dat proces is vaak behulpzaam bij het voorkomen van nieuwe klachten.
12.	Je hebt een foutmelding uit het elektronisch cliëntendossier terwijl je een gevoelige situatie aan het rapporteren bent. Je belt met de helpdesk en de helpdeskmedewerker wil je scherm overnemen.	Probeer of de situatie ook opgelost kan worden zonder dat de helpdeskmedewerker juist deze informatie onder ogen krijgt. Als dat niet lukt, dan is het onvermijdelijk dat de helpdeskmedewerker informatie te zien krijgt.



Dossier gluren		
13.	Je bent vrijwilliger bij de Zonnebloem. Op de komende reis gaat een cliënt van jouw zorginstelling mee. Met deze cliënt heb je geen behandelrelatie. Als voorbereiding op de reis neem je even zijn dossier door, zodat je hem goed kunt helpen.	Niet oké. Je hebt geen behandelrelatie met deze cliënt. Je krijgt via de Zonnebloem de benodigde informatie. Je kunt nagaan of de cliënt het op prijs stelt als je vooraf even op bezoek komt. Als je als vrijwilliger informatie krijgt mag dat niet meer zijn dan nodig. Krijg je wel meer, trek dan aan de bel.
14.	Een van je medewerkers moet zijn rapportagevaardigheden verbeteren. Als manager neem je de rapportages door die deze medewerker in verschillende dossiers heeft geschreven, om samen te kunnen bespreken hoe het beter kan.	Dit kan toegestaan zijn, afhankelijk van het beleid in jullie zorginstelling. Vraag dit na bij je leidinggevende of jullie Functionaris voor Gegevensbescherming. Wie dat is? Dat hoor je op de website van je organisatie te kunnen vinden bij het onderwerp: privacy. Zie ook de opmerkingen bij 4.
15.	Een collega is ziek geworden en zij is nu opgenomen als cliënt in de eigen zorginstelling. Jullie willen graag weten hoe het met haar gaat dus lees je het na in het dossier.	Niet oké. Als je wilt weten hoe het met haar gaat kun je dit aan haar zelf vragen. Spreek met de collega af wat wel en niet gedeeld mag worden binnen de groep.
16.	Je bent op zoek naar een dossier en je opent per ongeluk het dossier van iemand met dezelfde achternaam. Zodra je ontdekt dat het niet het goede dossier is, sluit je het weer.	Geen probleem. Deze actie is wel gelogd, maar daaruit zal blijken dat je het dossier weer gesloten hebt.



Privacyspel

Pionnen



Zo start je het spel



Als je je bericht
opgehaald hebt



Als je veilig mailen hebt
ingeschakeld

Privacy-quizvragen

1.	Is het een datalek als je een zorgplan naar de familie van een andere cliënt gestuurd hebt?	Ja dat is een datalek. Direct melden volgens jullie meldprocedure. Als je die niet kent, vraag dan na hoe je meldingen kunt doen.
2.	Moet je een kopie-paspoort van een cliënt opslaan in het ECD of mag dit juist niet?	Dit mag niet! Direct melden volgens jullie meldprocedure. Als je die niet kent, vraag dan na hoe je meldingen kunt doen. De instelling mag alleen kopieën van paspoort of ID hebben van medewerkers in loondienst. Dit is zelfs een wettelijke plicht. Is er nog een procedure waarin staat dat je een kopie moet maken van het paspoort van een cliënt? Trek dan aan de bel. Bij een nieuwe cliënt moet iemand in de organisatie wel aan de hand van het paspoort vaststellen dat de cliënt is wie hij/zij zegt te zijn. Je noteert in dat geval wel dat je de controle hebt uitgevoerd en het paspoortnummer, maar je maakt geen kopie.



Privacy-quizvragen

3.	Hoe lang moeten de medische gegevens in een cliëntendossier bewaard blijven na vertrek of overlijden van de cliënt?	Minimaal 20 jaar. Dit volgt uit de Wet op de geneeskundige behandelovereenkomst. Waarschijnlijk is er een archiveringsmatrix opgesteld waarin staat hoe lang gegevens bewaard blijven. En zijn er procedures om dat te handhaven. Dat kan nog heel lastig zijn, zeker als gegevens op veel plaatsen zijn opgeslagen (ECD, netwerkschijf, mailbox, papieren dossier, enzovoorts ...).
4.	Is het een datalek als een brief met vertrouwelijke gegevens geopend retour komt?	Ja, want je weet niet wie de gegevens heeft ingezien. Direct melden dus.
5.	Mag de secretaresse met het wachtwoord van haar manager personeelsmutaties goedkeuren?	Nee, je mag nooit werken met het wachtwoord van iemand anders. Als de secretaresse personeelsmutaties mag goedkeuren, dan moet de instelling regelen dat zij dat onder haar eigen account kan. Als de secretaresse dat niet mag, dan moet de manager het gewoon zelf doen. Als iemand met het wachtwoord van iemand anders werkt, sluiten de autorisaties blijkbaar niet aan bij de werkzaamheden. Bespreek dit met je leidinggevende.
6.	Mag je foto's van een cliënt op Facebook plaatsen?	Alleen als je hiervoor toestemming hebt van de cliënt of zijn/haar wettelijk vertegenwoordiger. Ga na hoe bij jullie het verkrijgen van toestemming is geregeld.
7.	Als een collega zich ziekmeldt, mag de manager dan vragen welke ziekte hij heeft?	Nee, hier zijn strenge regels voor. De manager mag alleen vragen wanneer de collega verwacht er weer te zijn en welke afspraken er verzet of overgenomen moeten worden.



Privacy-quizvragen

8.	De informatie op Baxterzakjes, gaat dat om persoonsgegevens? Ja of nee? Is het veilig om Baxterzakjes in de gewone prullenbak weg te gooien?	Dat zijn zeker persoonsgegevens. Het is niet veilig om deze in de gewone prullenbak te gooien. Hoe het wel moet is afhankelijk van de afspraken binnen jullie zorginstelling.
9.	Wat doe je als je vertrouwelijke gegevens op de printer vindt en er is niemand in de buurt?	Versnipperen of in de container om te vernietigen is het veiligst. Als je weet van wie het is kun je het ook aan die persoon geven en vragen of hij/zij het al kwijt was. Naar aanleiding van dit spel kunnen jullie in het team afspraken maken hoe je hiermee omgaat.
10.	Wat is een phishingmail en waaraan zou je die kunnen herkennen?	Phishing is een mail waarin bijvoorbeeld geprobeerd wordt informatie te krijgen (door je naar een inlogscherf te lokken) of kwaadaardige software te installeren. Je herkent dit o.a. aan links naar vreemde internetadressen, de vraag om in te loggen, een aanbod te mooi om waar te zijn.
11.	Mag je gegevens naar de gemeente sturen als ze daarom vragen, zoals een kopie-ID of een zorgdossier?	In sommige gevallen mag de gemeente informatie opvragen. Kijk goed welke afspraken er binnen jullie instelling zijn.
12.	Hoe lang mag je een sollicitatiebrief (op papier en digitaal) bewaren van iemand die niet is aangenomen?	Maximaal tot vier weken na het afsluiten van de procedure. Met toestemming van de sollicitant mag je de gegevens maximaal één jaar in portefeuille houden.



Privacy-quizvragen

13.	Wat is het belangrijkste om een wachtwoord veilig te maken? a) Dat het complex is dus met vreemde tekens als @#\$ erin en hoofdletters, kleine letters, cijfers b) Dat je het regelmatig wijzigt c) Dat het lang is d) Dat het een veel voorkomend wachtwoord is als 123456 of qwerty e) Dat je het makkelijk kunt onthouden f) Dat je het briefje waar je het opgeschreven hebt goed wegstopt en niet op het scherm plakt	Het belangrijkste is een lang wachtwoord van 12 karakters of meer. Dat is het moeilijkst om te kraken. Je kunt ook een wachtzin gebruiken.
14.	Waar moet je een melding maken als je een datalek (of iets wat daarop lijkt) hebt ontdekt?	Je hebt iets gezien, gehoord, gelezen wat misschien qua privacy of informatieveiligheid niet helemaal juist is. Soms twijfel je of je dit moet melden. Advies: altijd melden. Ga na hoe dit bij jullie geregeld is.
15.	Gebruik je voor het versturen van interne mail ook “veilig verzenden”? Moet je altijd “veilig verzenden” gebruiken bij het versturen van mail buiten de organisatie? Waarom wel/niet?	Intern is het niet nodig om “veilig verzenden” te gebruiken. Naar buiten is het alleen noodzakelijk als je vertrouwelijke informatie verstuurt. Zodra het informatie over personen is, is het vertrouwelijk.
16.	In de centrale hal hangen de naambordjes van alle bewoners van dit huis. Mag dat?	Dit kan zijn toegestaan, afhankelijk van het beleid in jullie zorginstelling.
17.	Is het toegestaan om overal in het elektronisch cliëntendossier (ECD) het BSN van de cliënt te zien?	Nee, het BSN is een extra gevoelig gegeven en mag alleen gebruikt worden waar dat wettelijk is voorgeschreven (bijv. bij declaraties).



Privacy-quizvragen

18.	Je zit in de trein en je hoort iemand vertellen over een woedeaanval van een cliënt die jij privé kent. Wat doe je? a) als je bij die vriend op bezoek gaat vertel je dit aan hem b) je staat op en gaat ergens anders zitten c) je spreekt de persoon aan d) je meldt het bij de Functionaris voor Gegevensbescherming (FG)	In ieder geval is melden bij de FG van de betreffende zorginstelling (d) een goede reactie, maar ook a) en c) zijn in dit geval op hun plaats.
19.	Je leest een rapportage in het elektronisch cliëntendossier (ECD) waar jouw naam onder staat, maar je hebt dat niet zelf geschreven. Wat doe je? a) je wachtwoord veranderen b) aan je collega's vragen wie dat geschreven heeft c) de rapportage wissen d) mail naar cliënt of familie sturen dat jij niet de auteur bent e) dit incident melden bij het meldpunt van jullie organisatie (bijvoorbeeld de Functionaris voor Gegevensbescherming of de servicedesk)	In ieder geval is melden (e) een goede reactie, maar ook a) en b) zijn in dit geval op hun plaats.
20	Familieleden willen graag foto's van de verjaardag van jouw cliënt via WhatsApp toegestuurd krijgen. Wat doe je?	WhatsApp op je telefoon hebben is onveilig: je geeft Facebook, de eigenaar van WhatsApp, hiermee toegang tot allerlei gegevens op jouw telefoon. Hoe je het wel oplost is afhankelijk van het beleid in jullie zorginstelling.



Bewaartermijnen

	Onderwerp		Bewaartermijn	
1.	medisch dossier	D	20 jaar na laatste wijziging in dossier	minimumtermijn
2.	personeelsdossier	G	2 jaar na einde dienstverband	maximumtermijn
3.	loonbelastingverklaring en kopie identiteitsbewijs	K	5 jaar na einde dienstverband	minimumtermijn
4.	salarisadministratie	A	7 jaar na einde dienstverband	minimumtermijn
5.	cameratoezicht	F	4 weken (tenzij nodig als bewijsmateriaal)	maximumtermijn
6.	sollicitatiebrieven (niet aangenomen)	C	4 weken na afsluiten procedure	maximumtermijn
7.	sollicitatiebrieven (in portefeuille)	I	1 jaar (alleen met toestemming van de betrokkene)	maximumtermijn
8.	verslag functioneringsgesprek	H	eigen beleid organisatie (maximaal 2 jaar na einde dienstverband)	
9.	niet-medisch en niet-financieel gedeelte van het zorgdossier	E	eigen beleid organisatie	
10.	medicatie-toedienlijsten	L	2 jaar (volgens IGJ) 2 maanden (volgens brancheverenigingen)	minimumtermijn
11.	loonbeslag	J	tot opheffing	maximumtermijn
12.	delen uit patiëntendossiers academische ziekenhuizen, zoals ontslagbrief en operatieverslag	B	115 jaar	minimumtermijn