Bewuste dossierinzage

Voorkom ongeoorloofde inzage in dossiers

Deze toolkit bevat uitleg, tips en hulpmiddelen om direct mee te starten

Informatieveilig gedrag in de zorg

Voorwoord

In de zorg staat vertrouwen hoog in het vaandel. Patiënten, cliënten en bewoners delen persoonlijke informatie in de verwachting dat daar zorgvuldig en respectvol mee wordt omgegaan. Toch komt het voor dat dossiers worden ingezien zonder dat daar een geldige reden voor is. Dat gebeurt niet alleen uit nieuwsgierigheid naar een bekende patiënt of cliënt. Denk bijvoorbeeld aan een medewerker die een dossier opent om te leren van een casus van een collega, na een overdracht wil weten hoe het met een patiënt of cliënt is afgelopen of uit betrokkenheid wil weten hoe een bekende patiënt of cliënt het maakt. Het ongeoorloofd inkijken van dossiers is een hardnekkig en multidimensionaal vraagstuk. Het raakt niet alleen aan privacy en wetgeving, maar ook aan professionele cultuur, bewustwording en menselijke afwegingen.

Juist omdat ongeoorloofde inzage vaak voortkomt uit oprechte en goedbedoelde intenties, is het onderwerp complex. Wat begint als leergierigheid of zorgzaamheid, kan onbedoeld leiden tot verlies van vertrouwen van degene die op ons rekenen voor veilige zorg. Ook kan het leiden tot een datalek en mogelijke reputatieschade voor de organisatie.

Regels en controle zijn niet voldoende om ongeoorloofde inzage te voorkomen. Het vraagt om kennis, bewustwording en het gesprek met elkaar over wat professioneel en zorgvuldig handelen betekent in de dagelijkse praktijk.

Deze toolkit biedt praktische hulpmiddelen om organisaties en teams in de zorg te ondersteunen bij het terugdringen van ongeoorloofde inzage in dossiers. De hulpmiddelen helpen bij het vergroten van kennis over privacy en dossierinzage, het creëren van bewustwording rondom intenties en grenzen, het stimuleren van ander gedrag en het voeren van open gesprekken binnen teams.

De toolkit is ontwikkeld voor CISO's, FG's, privacy officers en andere professionals die zich bezighouden met informatiebeveiliging en privacy. Zij kunnen de hulpmiddelen inzetten om binnen hun organisatie bewustwording te vergroten en het gesprek over zorgvuldig dossiergebruik te stimuleren.

De hulpmiddelen zijn ontwikkeld binnen het programma Informatieveilig gedrag in de zorg, in samenwerking met professionals uit het werkveld. Hun praktijkervaring, kennis en expertise zijn vertaald naar praktische hulpmiddelen die direct toepasbaar zijn binnen zorgorganisaties.

Alle hulpmiddelen uit deze toolkit zijn ook afzonderlijk te downloaden via **de website** van het programma Informatieveilig gedrag in de zorg.

We hopen dat deze hulpmiddelen jou en je collega's ondersteunen bij het voorkomen van ongeoorloofde inzage in dossiers.

Processchema

Ongeoorloofd inkijken dossiers

START

Je ontvangt een melding van ongeoorloofde inzage in een patiëntendossier

Hoe ontvang je een melding?

Handmatige controle

Waar kijk je naar?

Is de inzage verklaarbaar?

Ja en rechtmatig

Geen vervolgactie
Pas eventueel processen aan

Nee

Ja

Is verder onderzoek nodig?

Tip

Bewaartermijn gegevens intern onderzoek ongeoorloofde inzage

Verder onderzoek

Hoe pak je dit aan?

Wie doet dit?

Uitkomsten vervolgonderzoek

Nee

Tip

Voorbeelden van hoe je van onduidelijk meteen naar onrechtmatig gaat

Onduidelijk of het onrechtmatig was

Hoe kan dit?

Verklaarbaar en rechtmatig

Onrechtmatig

Interventie

Lees meer

Meld datalek

Lees meer

Informeer betrokkenen

Lees meer

GEREED

Leer en evalueer

Waar kijk je naar?

Terug naar figuur

Hoe ontvang je een melding?

Het startpunt van dit proces kan verschillend zijn, maar is altijd een ‘rode’ vlag die opgaat in een van de volgende situaties:

Loggingcontrole op basis van vastgestelde regels

Geautomatiseerde controles signaleren afwijkingen in het gebruik van dossiers, bijvoorbeeld inzage zonder behandelrelatie of opvallende patronen in toegang.

VOORBEELD Een verpleegkundige opent tijdens een spoedsituatie het dossier van een patiënt die onverwacht op de afdeling binnenkomt. Hiervoor gebruikt de verpleegkundige Breaking the Glass: een functie waarmee in uitzonderlijke situaties tijdelijk toegang kan worden verkregen tot een dossier zonder bestaande behandelrelatie. Deze inzage wordt altijd geregistreerd en kan automatisch worden gecontroleerd.

Steekproef

Periodieke of thematische controles van loggegevens brengen mogelijke onrechtmatige inzage aan het licht.

VOORBEELD Tijdens een periodieke controle bekijkt de privacy officer een aantal willekeurige inzagen. Daarbij valt op dat een medewerker regelmatig dossiers opent buiten de eigen afdeling. Dit is aanleiding om de inzagen nader te beoordelen.

Signaal intern of extern

Een melding van een medewerker, leidinggevende, patiënt of externe partij kan aanleiding zijn om het proces te starten. Wanneer een patiënt, cliënt of bewoner een melding doet, zorg er dan voor dat deze persoon gedurende het proces wordt geïnformeerd over de verschillende stappen die worden genomen.

VOORBEELD Een patiënt ziet in het inzagelog dat een onbekende medewerker het dossier heeft bekeken en vraagt de organisatie om uitleg. Deze melding kan aanleiding zijn om te onderzoeken of de inzage terecht was.

Terug naar figuur

Waar kijk je naar bij een handmatige controle?

Betrokken medewerker(s)

Welke medewerker heeft het dossier ingezien? Wat is de functie en rol binnen de organisatie?

Aard van de ingeziene informatie

Welke onderdelen van het dossier zijn bekeken? Denk aan medische gegevens, persoonlijke gegevens of rapportages.

Relatie tussen medewerker en patiënt

Is er een behandelrelatie, werkgerelateerde noodzaak of een privérelatie?

Aantal betrokken patiënten

Betreft het één of meerdere patiënten?

Frequentie van inzage

Hoe vaak is het dossier geraadpleegd (buiten de reguliere behandelrelatie)?

Incident of breder patroon

Gaat het om een eenmalige gebeurtenis of zijn er signalen dat dit vaker voorkomt, bv. binnen hetzelfde team of dezelfde afdeling?

Duur van de inzage

Hoe lang heeft de inzage per keer en in totaal plaatsgevonden?

Persoon en afdeling

Op welke afdeling werkt de medewerker en zijn daar eerder vergelijkbare signalen geweest?

Afsluitend oordeel vorming

Met de antwoorden op deze vragen krijg je een duidelijk beeld van wat er precies is gebeurd, wie erbij betrokken waren en hoe ernstig de situatie is. Door de antwoorden op bovenstaande vragen te combineren, kun je vaststellen of de inzage rechtmatig was of dat er sprake is van ongeoorloofd handelen.

Terug naar figuur

Hoe pak je verder onderzoek aan?

In deze stap voer je het onderzoek uit aan de hand van een logische volgorde. Gebruik deze volgorde als houvast, maar pas deze waar nodig aan de situatie aan. Zie de onderdelen niet als vaste stappen, maar als samenhangende aandachtspunten. Gebruik de vragen als inspiratie en ondersteuning bij het onderzoek en vorm daarbij steeds een inhoudelijk oordeel.
Op basis van de antwoorden kom je tot een gemotiveerde conclusie.

1. Start van het onderzoek
Welke melding is ontvangen en wat waren de bevindingen uit de eerste controle? Wat is de aanleiding voor verdiepend onderzoek? Wie is aangewezen als onderzoeksverantwoordelijke, bijvoorbeeld privacy officer of compliance functionaris?

2. Veiligstellen van relevante gegevens
Welke logbestanden, toegangsgegevens en systeeminformatie zijn relevant? Zijn deze veiliggesteld en opgeslagen om wijziging of verlies te voorkomen?

3. Analyse van loggegevens
Wat laten de toegangslogs zien over een ruimere periode?
Zijn er vergelijkbare inzagen in andere dossiers? Zijn er afwijkende patronen in tijdstippen of locaties zichtbaar?

4. Dossieranalyse
Zijn er indirecte behandelrelaties of andere werkgerelateerde verklaringen die in de eerste controle niet zichtbaar waren?
Sluiten werkzaamheden of caseload de inzage alsnog uit of juist aan?

5. Hoor en wederhoor
Wat is de toelichting van de betrokken medewerker op de inzage, werksituatie en context? Bekijk ook de infographic '**Hoe voer je een onderzoekend gesprek uit?**' uit deze toolkit.

6. Toetsing aan beleid en autorisaties
Is de medewerker correct geautoriseerd voor de ingeziene gegevens? Past de inzage binnen interne protocollen en gedragscode? Is er mogelijk sprake van tekortschietend autorisatiebeheer of procesfouten?

7. Beoordeling van ernst en impact
Hoe gevoelig zijn de ingeziene gegevens?
Hoeveel patiënten zijn betrokken?
Is er sprake van een datalek in de zin van de AVG?

8. Besluitvorming
Is vastgesteld dat sprake is van ongeoorloofde inzage?
Welke maatregelen zijn passend, zoals een waarschuwing, aanvullende scholing of een disciplinaire maatregel?

9. Vastleggen van conclusies
Zijn bevindingen, beoordeling en besluitvorming volledig en navolgbaar vastgelegd in een onderzoeksrapport?

Terug naar figuur

Wie pakt het verdere onderzoek op?

Uitgangspunt is dat het onderzoek zorgvuldig, objectief en aantoonbaar onafhankelijk wordt uitgevoerd door een persoon of team die zowel inhoudelijk als hiërarchisch op afstand staat van de betrokken medewerker en afdeling. Deze persoon beschikt over kennis van privacy, informatiebeveiliging en onderzoeksvaardigheden. Dit kan bijvoorbeeld een privacy officer, security officer, compliance officer of een externe zijn die is getraind in het uitvoeren van onderzoek.

Andere functies die kunnen bijdragen aan het onderzoek:

HR
HR ondersteunt bij arbeidsrechtelijke aspecten, dossiervorming en eventuele maatregelen richting de medewerker.

IT
Levert technische ondersteuning bij het veiligstellen en analyseren van loggegevens en autorisaties.

Direct leidinggevende
De leidinggevende levert feitelijke context over functie, taken en werkafspraken, maar voert niet zelf het onderzoek uit om belangenverstrengeling te voorkomen.

Leverancier van het EPD of systeem
Wordt betrokken wanneer aanvullende technische analyse nodig is of wanneer loggegevens nader moeten worden geduid.

Juridische afdeling
Adviseert over privacywetgeving, meldplicht datalekken, proportionaliteit van maatregelen en juridische risico's.

Andere afdeling of externe partij
Indien nodig kan een andere afdeling of externe onderzoeksinstantie worden ingeschakeld om de onafhankelijkheid te waarborgen, bijvoorbeeld bij signalen van een breder patroon binnen één team.

Terug naar figuur

Voorbeelden van hoe dit kan

In sommige situaties laten deze gegevens zodanig duidelijke afwijkingen zien dat de inzage niet te verklaren is vanuit functie, planning of zorgproces. Onderstaande voorbeelden zijn situaties waarin op basis van beschikbare data onrechtmatige inzage waarschijnlijk lijkt.

Dossier van een patiënt (bijvoorbeeld een directe collega, familielid, BN'er) is meerdere keren geraadpleegd terwijl er geen behandelrelatie of betrokkenheid vanuit de functie van de medewerker.

Een groot aantal dossiers van patiënten buiten de eigen afdeling zijn geopend zonder dat de medewerker een consult, overdracht of ondersteunende taak had.

Het dossier is herhaaldelijk geopend over een langere periode zonder registratie van zorgactiviteiten, rapportages of andere werkgerelateerde handelingen en/of behandelrelatie.

Terug naar figuur

Voorbeelden van hoe dit kan

Bijvoorbeeld:

Na een melding van inzage zonder behandelrelatie blijkt uit het log dat dit plaatsvond tijdens een dienst met afdelingsbrede administratieve taken. Door ontbrekende of onvolledige documentatie en het ontbreken van bevestiging door collega's blijft onduidelijk of de inzage rechtmatig was.

Inzage vond plaats tijdens een drukke dienst met meerdere patiëntoverdrachten, maar door gebrekkige registratie van taken en overdrachten kan niet worden vastgesteld of er een functionele reden was.

Terug naar figuur

Afhandelen van datalek

Gebruik de **toolkit melden datalek** voor wie extern geïnformeerd moet worden. Intern breng je selectief de juiste partijen op de hoogte, afhankelijk van de aard en impact van het incident:

Raad van Bestuur
Vanwege de bestuurlijke eindverantwoordelijkheid voor privacy, risicobeheersing en besluitvorming over eventuele vervolgstappen.

Raad van Toezicht
Vanuit hun toezichthoudende rol op goed bestuur, naleving van wetgeving en beheersing van organisatie risico's.

Ondernemingsraad
Omdat het incident gevolgen kan hebben voor medewerkers en kan leiden tot aanpassingen in beleid, procedures of controles.

Functionaris Gegevensbescherming
Voor onafhankelijke toetsing aan de AVG, advies over meldplicht en borging van correcte afhandeling.

Communicatieafdeling
Ter voorbereiding op mogelijke vragen van patiënten, media of andere externe partijen en voor eenduidige communicatie.

Terug naar figuur

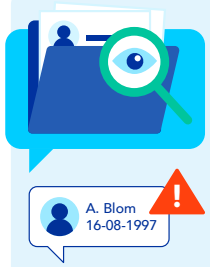
Interventies

Een passende interventie is altijd afhankelijk van de situatie en de organisatie. Daarom geven wij hiervoor geen vast advies. Mogelijke interventies lopen uiteen van een gesprek met een medewerker of een team, tot aanvullende training, een waarschuwing of, in het uiterste geval, ontslag. Welke interventie passend is, hangt altijd af van de specifieke omstandigheden.

Terug naar figuur

Informeer betrokkenen

Informeer de betrokken medewerker(s) over de uitkomsten van het onderzoek, de eventuele consequenties en de vervolgstappen, ook als de inzage rechtmatig is bevonden, zodat de medewerker duidelijkheid krijgt.



Licht de betrokken patiënt(en), cliënt(en) en/of bewoner(s) toe wat er is gebeurd, welke gegevens ongeoorloofd zijn ingezien, welke bevindingen het onderzoek heeft opgeleverd en welke gevolgen dit mogelijk voor hen heeft. Leg uit welke maatregelen de organisatie heeft genomen om het incident af te handelen en herhaling te voorkomen. Bied betrokkenen de mogelijkheid om vragen te stellen en wijs hen op een contactpersoon voor eventuele vervolgvragen.

Leg vast welke personen zijn geïnformeerd en wanneer de terugkoppeling heeft plaatsgevonden. Indien sprake is van een melding aan de Autoriteit Persoonsgegevens, leg dan tevens vast hoe de betrokkene(n) zijn geïnformeerd, zodat deze informatie kan worden opgenomen in de melding.

Komt uit het aanvullende onderzoek naar voren dat de inzage rechtmatig was, of dat niet kan worden vastgesteld of de inzage rechtmatig was, informeer dan altijd de medewerker. Op die manier krijgt de medewerker duidelijkheid over de uitkomst van het onderzoek. De patiënt, cliënt of bewoner hoeft hierover niet te worden geïnformeerd.

Terug naar figuur

Bewaartermijn gegevens intern onderzoek ongeoorloofde inzage

Bij een melding van ongeoorloofde inzage worden persoonsgegevens verwerkt van medewerkers en mogelijk van patiënten. Voor deze gegevens geldt geen afzonderlijke wettelijke bewaartermijn. De organisatie bepaalt de bewaartermijn op basis van de Algemene verordening gegevensbescherming.

Juridisch kader

Volgens artikel 5 lid 1 sub E van de AVG mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor zij zijn verzameld. De bewaartermijn moet daarom:

- doelgebonden zijn
- proportioneel zijn
- vastgelegd zijn in het interne bewaarbeleid

Uitwerking per type gegevens

1. Onderzoeksdossier medewerker

Gegevens uit het interne onderzoek worden bewaard zolang dat nodig is voor:

- afronding van het onderzoek
- eventuele arbeidsrechtelijke maatregelen
- mogelijke juridische procedures

Gebruikelijke termijn:

- 2 jaar na afronding van het onderzoek
- verlenging tot maximaal 5 jaar indien juridische procedures te verwachten zijn

Onderbouwing:

- Artikel 5 lid 1 sub e AVG
- Artikel 3:307 Burgerlijk Wetboek, verjaringstermijn 5 jaar

2. Loggegevens inzage patiëntendossier

Loggegevens vallen onder NEN 7513.
Deze norm schrijft voor dat logginggegevens minimaal 5 jaar worden bewaard.

3. Gegevens opgenomen in het medisch dossier

Indien informatie uit het onderzoek wordt toegevoegd aan het patiëntendossier, geldt de bewaartermijn van de WGBO:

- 20 jaar vanaf de laatste wijziging van het dossier
- Artikel 7:454 Burgerlijk Wetboek

VOORWAARDE De organisatie legt de gekozen bewaartermijnen vast in het bewaarbeleid en zorgt voor passende beveiliging conform artikel 32 AVG.

Terug naar figuur

Leer en evalueer

Niet alleen directe fouten corrigeren, maar ook dieperliggende aannames, normen en waarden onderzoeken die bijdroegen aan de ongeoorloofde inzage. Dit doe je door:

Maak van iedere melding een structureel leermoment

VOORBEELD Voeg het bespreken van privacy-incidenten toe aan vaste agendapunten in teamvergaderingen. Gebruik anonimiseerde casussen als leermateriaal in trainingen en evalueer jaarlijks het effect van de maatregelen.

Bespreek leerpunten veilig en anoniem binnen teams

VOORBEELD Organiseer een “veilige” reflectiesessie, bijvoorbeeld met een externe gespreksleider, waar medewerkers zonder angst voor gevolgen kunnen delen wat zij hebben geleerd. Maak hierbij gebruik van casuïstiek uit de praktijk.

Verzamel en bundel feiten, oorzaken en patronen

VOORBEELD Stel een multidisciplinair team samen (bijv. compliance, HR, IT, zorgverleners) om alle bevindingen uit de melding te documenteren in een gestructureerd rapport. Gebruik hiervoor een vast format, zoals een SWOT-analyse of een fishbone-diagram, om oorzaken en patronen inzichtelijk te maken.

Verwerk inzichten in beleid, systeeminrichting en scholing

VOORBEELD Pas het privacybeleid aan op basis van de bevindingen, bijvoorbeeld door strengere autorisatieregels of extra controles in te voeren. Ontwikkel een gerichte training over ethisch handelen en privacybewustzijn, en maak deze verplicht voor alle medewerkers.

Analyseer op drie niveaus: medewerker, team en organisatie

VOORBEELD Organiseer gesprekken met betrokken medewerkers, teamleiders en afdelingshoofden. Gebruik vragenlijsten of interviews om inzicht te krijgen in individuele motieven, teamdynamieken en organisatiecultuur. Maak gebruik van anonimiteit om openheid te stimuleren.

Koppel zichtbaar terug wat er is verbeterd

VOORBEELD Communiceer de genomen maatregelen en verbeteringen via interne kanalen (nieuwsbrief, intranet) en in teamoverleggen. Laat zien hoe meldingen hebben geleid tot concrete veranderingen, bijvoorbeeld door voor- en na-situaties te presenteren.

Onderzoek achterliggende factoren

VOORBEELD Voer een risicoanalyse uit naar kennisniveaus (bijv. privacybewustzijn), cultuur (bijv. “wij-cultuur” vs. verantwoordelijkheidsgevoel), autorisaties (wie heeft toegang tot welke gegevens?) en werkdruk (tijdsdruk, onderbezetting). Gebruik tools zoals een cultuurscan of werkdrukanalyse.

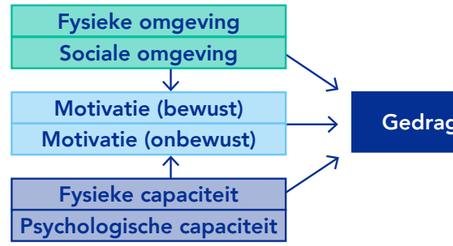
Knelpuntenanalyse

Probleem (risico)	Zorgmedewerker kijkt ongeoorloofd in het dossier van patiënt, cliënt of bewoner en veroorzaakt reputatie- en vertrouwensschade.
Doelgedrag	De zorgmedewerker raadpleegt gegevens in het dossier alleen wanneer dit noodzakelijk is, beperkt zich tot gegevens die relevant zijn en sluit het dossier direct na gebruik.
Doelgroep	Zorgmedewerkers (ZM): zorgprofessionals en andere werknemers binnen een zorgorganisatie.

Deze knelpuntenanalyse is opgebouwd volgens het COM-B model en helpt je te begrijpen waardoor ongewenst gedrag, zoals ongeoorloofde inzage in dossiers, ontstaat. De knelpuntenanalyse laat de meest voorkomende oorzaken van ongeoorloofde inzage in dossiers zien.

Begin met de knelpunten die je herkent binnen jouw organisatie of team. Gebruik de analyse ook als hulpmiddel tijdens gesprekken met collega's. Bespreek samen welke knelpunten spelen, waardoor deze ontstaan en welke acties kunnen helpen om ongeoorloofde inzage te voorkomen.

COM-B model — Stap 3 uit De Wegwijzer



- Oorzaak om product op te ontwikkelen
- Hulpmiddel melden datalek

Doelgedrag
De zorgmedewerker raadpleegt informatie alleen wanneer dit noodzakelijk is, beperkt zich tot gegevens die relevant zijn en sluit het dossier direct na gebruik.

Fysieke omgeving / Sociale omgeving

- Dossier/EPD is niet goed afgesloten waardoor iedereen op die werkplek erbij kan
  - Scherm niet gelocked
    - Systeem niet goed ingeregeld
      - Gebruiksgemak gaat boven veiligheid
        - Er is geen beleid in de organisatie
        - Beleid wordt niet nageleefd
          - Bestuur, RvT en leidinggevende zien hier niet op toe
- Tijdelijke rechten blijven langer bestaan dan nodig
  - Geen monitoring
- Andere collega's doen het ook
  - Geen goed trainings- en scholingsaanbod beschikbaar
  - Informatie is verspreid en lastig terug te vinden
    - Belang van training voor ZM wordt door organisatie niet ingezien
  - Cultuur waarin mee-kijken in dossiers als normaal of onschuldig wordt gezien
    - Geen aandacht in onboarding en geen herhaling van onderwerp daarna
  - Er is geen positieve sociale invloed
    - Geen duidelijk meldproces/ medewerker weet niet waar melding van ongewenst gedrag te maken
    - Geen voorbeeld-gedrag en verkeerde onderliggende normen en waarden
- Tijds-/werkdruk waardoor per abuis verkeerd dossier wordt geopend
- Terugkoppeling gebeurt vooral bij incidenten en dan vooral corrigerend
  - Weinig voorbeelden van datalekken gaan over ongeoorloofd inkijken in dossiers
  - Medewerkers merken geen handhaving op ongeoorloofd inzagen in dossiers
  - Leren gebeurt op de werkvloer door afkijken: 'iedereen doet het zo'
  - Geen sancties
  - Geen sanctiebeleid

Motivatie (bewust) / Motivatie (onbewust)

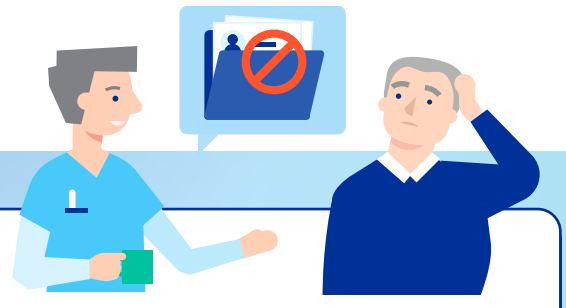
- ZM ziet inzage als onschuldige handeling
  - Geen duidelijkheid over de gevolgen
    - De gevolgen zijn te weinig voelbaar om gedrag te sturen
  - Onbekendheid over dat het niet mag volgens wet- en regelgeving
  - Desinteresse in het onderwerp
- ZM verwacht weinig kans op ontdekking
  - ZM gelooft dat niemand er last van heeft als je niets doorvertelt
    - Ik word toch niet betrapt
      - Onvoldoende risico inschatting
        - Er is onvoldoende oog voor schade voor de organisatie
        - Er is onvoldoende oog voor persoonlijke schade voor de cliënt
- ZM zoekt bewust voor eigen gewin informatie op
- Inkijken in dossiers is gewoonte geworden
  - Medewerker maakt geen onderscheid tussen professionele noodzaak en persoonlijke nieuwsgierigheid
    - Inzage voelt als een neutrale handeling

Fysieke capaciteit / Psychologische capaciteit

- ZM herkent het risicomoment niet
  - ZM weet niet wat en dat het een datalek is
    - Gebrek aan kennis over regelgeving
      - ZM weet niet dat scholingsaanbod binnen organisatie bestaat
- ZM weet het verschil tussen betrokkenheid en rechtmatig niet
  - Medewerker weet niet wanneer inkijken (on)geoorloofd is

Ongeoorloofde dossierinzage:
Aandachtspunten voor een onderzoekend gesprek

Deze infographic helpt leidinggevenden en experts informatieveiligheid bij het voeren van een onderzoekend gesprek met een medewerker na ongeoorloofd inkijken in een dossier.



1 Voorbereiding

Zorg dat je goed voorbereid het gesprek ingaat.

Voor het gesprek:

- Doorloop het eerste deel van het processchema en verzamel feiten zoals loggegevens.
- Bepaal vooraf welke vragen je wilt stellen.
- Zorg voor een rustige en vertrouwelijke gespreksomgeving.
- Denk goed na over of, en zo ja wie, je uitnodigt voor het gesprek. Bij een onderzoekend gesprek kan het voor een medewerker onprettig of intimiderend overkomen wanneer er meerdere mensen tegenover hem of haar zitten.

2 Zo pak jij je rol als gespreksleider

Een onderzoekend gesprek vraagt om een open, professionele en reflectieve houding. De manier waarop de gespreksleider het gesprek voert, bepaalt in sterke mate of een medewerker zich veilig voelt om open te vertellen wat er is gebeurd. Door actief te luisteren, samen te vatten en door te vragen ontstaat ruimte om niet alleen het incident te bespreken, maar ook de onderliggende oorzaken beter te begrijpen.

Tips voor een goed gesprek

Transparant
- Leg uit waarom het gesprek plaatsvindt.
- Maak het doel van het gesprek duidelijk.
- Vertel vooraf dat je aantekeningen maakt van het gesprek en wat je met die aantekeningen doet.

Respectvol en veilig
- Creëer een veilige sfeer.
- Blijf rustig en professioneel.

Reflectief
- Stimuleer de medewerker om mee te denken.
- Vraag ook wat de organisatie beter kan doen. Zo leren jullie allebei van het gesprek.

Open en nieuwsgierig
- Probeer te begrijpen wat er gebeurde.
- Stel open vragen.

3 Stappen van het gesprek

1. Doel van het gesprek uitleggen

Leg uit dat het doel van het gesprek is om samen te begrijpen wat er is gebeurd en waarom. Benadruk dat het gesprek bedoeld is om ervan te leren en om te kijken hoe een vergelijkbare situatie in de toekomst kan worden voorkomen. Later in het gesprek kun je, als dat nodig is, ingaan op het belang van vertrouwelijkheid en privacy in de zorg.

Voorbeeldformulering:
"Ik wil vandaag met je in gesprek om goed te begrijpen wat er is gebeurd en wat de context was. Het is belangrijk dat we zorgvuldig omgaan met patiëntgegevens. Dit gesprek is bedoeld om te onderzoeken en te leren, niet om te oordelen."

2. Context verkennen

Stel open vragen om te begrijpen wat er is gebeurd. Bespreek de reden van het inkijken van het dossier en onderzoek of er een functionele noodzaak of behandelrelatie was. Geef de medewerker ruimte om de situatie toe te lichten en bespreek ook omstandigheden die mogelijk invloed hebben gehad op de beslissing.

Voorbeeldvragen:
"Kun je mij meenemen in wat er die dag gebeurde?"
"Wat was voor jou de aanleiding om het dossier te openen?"
"Wat was op dat moment jouw rol of betrokkenheid?"
"Was er een behandelrelatie of functionele noodzaak?"
"Waren er omstandigheden die invloed hadden op jouw beslissing?"
"Welke afweging maakte je op dat moment?"

3. Uitleg geven over richtlijnen en verwachtingen

Leg uit wat de interne richtlijnen zijn rondom toegang tot en gebruik van patiëntgegevens. Verwijs naar professionele normen, interne gedragscodes en privacyregels, zoals de AVG en beroepscodes. Licht toe dat onbevoegd inkijken de privacy van patiënten kan schaden en het vertrouwen in de organisatie kan aantasten.

Voor reflectieve vragen:
"Hoe kijk je hier zelf op terug?"
"Als je nu terugkijkt, zou je iets anders doen?"
"Hoe kijk je naar onze richtlijnen?"
"Wat betekent vertrouwelijkheid voor jou in je werk?"

4. Afronding van het gesprek

Vat samen wat besproken is. Vraag wat de medewerker meeneemt uit dit gesprek en vraag ook om tips voor de organisatie. Bespreek vervolgstappen en afspraken.

4 Vastleggen en vervolg

Leg feiten en antwoorden zorgvuldig vast
- Noteer afspraken en vervolgstappen.
- Vermijd het opnemen van privacygevoelige informatie.
- Gebruik inzichten voor verdere beoordeling en om processen of systemen te verbeteren.

Samen zorgen voor veilige inzage

De belangrijkste afspraken op een rij

Do's

- ✔ **Handel met een duidelijk doel:** Raadpleeg patiëntgegevens alleen als het direct bijdraagt aan de behandeling, veiligheid of zorg van de patiënt, of als de wet dit vereist. Weeg altijd af of het inkijken echt noodzakelijk is en of het het belang van de patiënt dient.

  Stel jezelf vooraf de vraag: wat is mijn doel en kan ik dit ook bereiken zonder het dossier te openen?

- ✔ **Vraag om advies bij onduidelijkheid:** Twijfel je of toegang tot een dossier geoorloofd is? Vraag het dan eerst na.

  Vraag advies aan een collega. Kom je er samen niet uit? Benader dan jouw leidinggevende, of neem contact op met de verantwoordelijke voor informatieveiligheid in jouw organisatie. Zij kunnen helpen een weloverwogen beslissing te nemen.

- ✔ **Meld en leer van onbedoelde toegang:** Open je per ongeluk of onterecht een verkeerd dossier en heb je persoonlijke informatie gelezen? Meld dit bij jouw leidinggevende. Samen beoordelen jullie of jullie het datalek moeten melden en of verdere stappen nodig zijn. Zo verbeteren we de veiligheid en leren we als team.

  Meld het zo snel mogelijk, wees open over wat er is gebeurd en leg vast wat je hebt gezien. Bespreek samen hoe dit in de toekomst voorkomen kan worden.

- ✔ **Gebruik geanonimiseerde voorbeelden om van te leren:** Wil je je professionele kennis vergroten? Gebruik dan geanonimiseerde casussen of vraag toestemming aan een cliënt om dossiers te raadplegen voor opleidingsdoeleinden.

  Verwijder alle herleidbare gegevens of bespreek casussen op hoofdlijnen. Vraag vooraf toestemming aan de desbetreffende cliënt als je echte dossiers wilt gebruiken voor leerdoeleinden en check of dit binnen de afspraken van de organisatie past. Maak hiervan een notitie in het dossier van de cliënt.

Don'ts

- ✖ **Neuzen in gegevens uit nieuwsgierigheid:** Kijk nooit in een dossier uit bezorgdheid, emotionele betrokkenheid of nieuwsgierigheid van een patiënt waar je geen behandelrelatie mee hebt. Ook niet als je een hechte band met de patiënt hebt (gehad).

  Zoek steun bij collega's of een vertrouwenspersoon als je emotioneel geraakt wordt, of vraag een betrokken collega hoe het met de cliënt gaat of is gegaan.

- ✖ **Gegevens delen zonder noodzaak:** Verspreid patiëntinformatie niet naar collega's of anderen, tenzij dit direct nodig is voor de zorg of behandeling van de patiënt.

  Stel jezelf vooraf de vraag: draagt dit direct bij aan de zorg voor deze patiënt? Zo niet, deel de informatie niet en bespreek algemene vragen zonder herleidbare details.

- ✖ **Buiten je rol handelen:** Raadpleeg geen dossiers van patiënten die je niet behandelt, zelfs niet als je denkt dat het je eigen patiënten ten goede komt.

  Zoek alternatieven, zoals overleg met de behandelend professional of naslagwerken.

- ✖ **Wensen van de patiënt negeren:** Als een patiënt heeft aangegeven dat bepaalde informatie niet gedeeld mag worden, respecteer die wens.

  Controleer actief de vastgelegde voorkeuren van de patiënt en overleg bij twijfel met je leidinggevende of de privacyfunctionaris voordat je informatie deelt.

Presentatietemplate

Het presentatietemplate bevat een voorbeeldpresentatie over ongeoorloofde inzage in dossiers. Deze presentatie helpt teamleiders en medewerkers om binnen hun team het gesprek te voeren over het wel en niet toegestaan inkijken van dossiers. Om te voorkomen dat medewerkers in dossiers kijken terwijl dat niet mag, is het belangrijk dat je werkt aan vertrouwen, professionaliteit en zorgvuldigheid. Besteed hier daarom aandacht aan vóórdat er incidenten ontstaan. Door er samen bewust bij stil te staan, creëer je duidelijkheid over wat binnen de organisatie als passend gedrag wordt gezien.

De presentatie behandelt de belangrijkste aandachtspunten die je met collega's kunt bespreken en bevat verschillende voorbeelddilemma's om het gesprek op gang te brengen. Daarnaast kun je de presentatie aanvullen met een eigen dilemma of praktijkvoorbeeld uit de organisatie, zodat deze beter aansluit bij jullie dagelijkse praktijk.

Per slide is in de notities een toelichting opgenomen die je kunt gebruiken tijdens het presenteren.

Colofon

De toolkit ‘Bewuste dossierinzage’ is een uitgave van het programma Informatieveilig gedrag in de zorg.

Het programma Informatieveilig gedrag in de zorg wordt uitgevoerd door stichting ECP | Platform voor de Informatiesamenleving in opdracht van het ministerie van VWS. De brancheorganisaties ActiZ, de Nederlandse ggz, NFU, NVZ, UMCNL en VGN zijn bij het programma betrokken.

Auteurs
Sebastiaan Stam, ECP | Platform voor de Informatiesamenleving
Mara van Heffen, ECP | Platform voor de Informatiesamenleving
Mariët de Waal, ECP | Platform voor de Informatiesamenleving

Communicatie
Demi van Spronssen, ECP | Platform voor de Informatiesamenleving
Djuly Kattenburg, ECP | Platform voor de Informatiesamenleving

In samenwerking met werkgroep Bewuste dossierinzage

Annelou Stehouwer	Functionaris Gegevensbescherming / Data Protection Officer – Waardeburgh
Daymian Vos	Adviseur Informatiebeveiliging en Privacy – Beweging 3.0
Ellen van Broekhoven-Grutters	Juridisch Beleidsadviseur en Functionaris Gegevensbescherming – ZZG zorggroep
Evelien Kruisselbrink	Coördinerend Privacy Officer – UMC Utrecht
Jan Willem Schoemaker	Chief Information Security Officer – Erasmus MC
Linda van de Sande	Senior Compliance Officer – Erasmus MC
Marleen van Aartrijk	Informatiemanager / Producteigenaar ONS – Visio
Nicole Suurland	Privacyjurist – Erasmus MC

Meelezers

Dominique Booms	Chief Privacy Officer – Erasmus MC
Eric Consten	Senior Privacy Officer – Ipse de Bruggen
Janneke Brandwijk	Informatieadviseur Cyber Security – Pieter van Foreest
Femke Agtersloot	Adviseur Beleid, Kwaliteit & Innovatie / Privacy Officer – Prinsenstichting
Marit Buijs	Strategisch Beleidsadviseur en Coördinator Data & Analyse – Erasmus MC