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 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

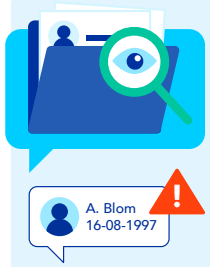
Interventies

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.