

Privacy en informatiebeveiliging:

Wat regelt HCl en wat is de verantwoordelijkheid van jouw praktijk?

Duidelijkheid over dataverwerking en verantwoordelijkheden

Privacy en informatiebeveiliging zijn belangrijke onderwerpen binnen de zorg. We ontvangen regelmatig vragen van praktijken over de verwerking van persoonsgegevens, de verwerkersovereenkomst en de verantwoordelijkheden van HCl en de praktijk.

Mede door ontwikkelingen op het gebied van wet- en regelgeving, zoals de NIS2-richtlijn, neemt de aandacht voor deze onderwerpen verder toe.

Om duidelijkheid te bieden, beantwoorden we hieronder de meest gestelde vragen over dataverwerking, informatiebeveiliging en de verdeling van verantwoordelijkheden.

1. Wie is verantwoordelijk voor patiëntgegevens?

Bij de verwerking van patiëntgegevens hebben de praktijk en HCl ieder een eigen rol en verantwoordelijkheid.

De praktijk is verwerkingsverantwoordelijke.

Dit betekent dat de praktijk verantwoordelijk is voor:

- Het bepalen van het doel en de middelen van de verwerking van persoonsgegevens.
- Het correct instellen en beheren van gebruikersrechten en autorisaties.
- Het zorgvuldig omgaan met patiëntgegevens.
- Het naleven van privacywetgeving en het waarborgen van de rechten van patiënten.

HCl treedt op als verwerker.

Dit betekent dat HCl:

- Persoonsgegevens uitsluitend verwerkt in opdracht van de praktijk.
- Passende technische en organisatorische beveiligingsmaatregelen treft.
- De praktijk waar nodig ondersteunt bij privacyvraagstukken, datalekken en verzoeken van patiënten.

Privacy en informatiebeveiliging zijn daarmee een gezamenlijke verantwoordelijkheid, waarbij beide partijen hun eigen verplichtingen hebben.

2. Wat doet HCI met persoonsgegevens?

HCI verwerkt persoonsgegevens uitsluitend voor zover dit noodzakelijk is voor het leveren en ondersteunen van haar dienstverlening.

Hierbij gelden de volgende uitgangspunten:

- Persoonsgegevens worden uitsluitend verwerkt volgens de afspraken en instructies van de praktijk.
- De verwerking vindt plaats overeenkomstig de geldende verwerkersovereenkomst.
- HCI gebruikt patiëntgegevens niet voor eigen doeleinden.

3. Wie is verantwoordelijk bij een datalek?

Bij een beveiligingsincident of datalek binnen de dienstverlening van HCI gelden de volgende verantwoordelijkheden:

- **HCI:** informeert de betreffende praktijk zo snel mogelijk zodra een datalek is vastgesteld en ondersteunt bij het onderzoeken en afhandelen van het incident.
- **De praktijk:** beoordeelt of het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens en/of de betrokken patiënten.
- **HCI en de praktijk:** werken waar nodig samen om de gevolgen van het incident te beperken en herhaling te voorkomen.

De praktijk blijft als verwerkingsverantwoordelijke verantwoordelijk voor het beoordelen en afhandelen van eventuele meldverplichtingen.

4. Welke verantwoordelijkheden heeft de praktijk zelf?

Naast de beveiligingsmaatregelen die HCI treft, heeft de praktijk ook eigen verplichtingen op het gebied van privacy en informatiebeveiliging.

De praktijk is onder andere verantwoordelijk voor:

- Het beschikken over een geldige grondslag voor de verwerking van persoonsgegevens.
- Het beheren van gebruikersaccounts, toegangsrechten en autorisaties.
- Het opstellen en naleven van interne privacy- en beveiligingsprocedures.
- Het zorgvuldig omgaan met persoonsgegevens binnen de eigen organisatie.
- Het behandelen van verzoeken van patiënten, zoals inzage, correctie of verwijdering van gegevens.

5. Hoe zorgt HCI voor informatiebeveiliging?

HCI besteedt structureel aandacht aan de bescherming van persoonsgegevens en de beveiliging van haar systemen.

Hiervoor worden verschillende technische en organisatorische maatregelen getroffen, waaronder:

- Toegangsbeheer en autorisaties.
- Beveiligde verbindingen en versleuteling van gegevens.
- Periodieke controles en audits.
- Bewustwording en training van medewerkers.

Meer informatie over onze aanpak vind je op onze website:

[HCI Informatiebeveiliging](#)

6. Maakt HCI gebruik van subverwerkers?

Ja, voor bepaalde onderdelen van onze dienstverlening kan HCI gebruikmaken van externe partijen die als subverwerker optreden.

Hierbij gelden duidelijke voorwaarden:

- Subverwerkers moeten voldoen aan de toepasselijke privacy- en beveiligingseisen.
- Er worden passende contractuele afspraken gemaakt over de verwerking en bescherming van persoonsgegevens.
- Praktijken hebben recht op inzicht in de inzet van subverwerkers.
- De afspraken hierover zijn vastgelegd in de verwerkersovereenkomst.

7. Wie behandelt verzoeken van patiënten?

De praktijk is het eerste aanspreekpunt voor patiënten die vragen hebben over hun persoonsgegevens.

Dit geldt bijvoorbeeld voor verzoeken tot:

- Inzage in persoonsgegevens.
- Correctie van onjuiste gegevens.
- Verwijdering van persoonsgegevens, voor zover wettelijk toegestaan.

HCI kan de praktijk waar nodig ondersteunen bij de technische uitvoering van dergelijke verzoeken.

De verantwoordelijkheid voor de beoordeling en afhandeling blijft bij de praktijk.

8. Wat betekent NIS2 voor de praktijk?

De Europese NIS2-richtlijn stelt strengere eisen aan de digitale weerbaarheid en informatiebeveiliging van organisaties die onder deze regelgeving vallen.

Belangrijke aandachtspunten zijn:

- Het treffen van passende beveiligingsmaatregelen.
- Het aantoonbaar beheersen van cyberrisico's.
- Het zorgvuldig omgaan met beveiligingsincidenten.
- Het waarborgen van informatiebeveiliging binnen de leveranciersketen.

Of en in welke mate de verplichtingen van toepassing zijn, hangt af van de situatie en de wettelijke kwalificatie van de betreffende organisatie.

Ongeacht de wettelijke verplichtingen blijft het belangrijk dat zowel HCl als de praktijk aandacht besteden aan digitale veiligheid en het voortdurend verbeteren van beveiligingsmaatregelen.

9. Kan de praktijk gebruikmaken van de cyberverzekering van HCl?

Nee, de cyberverzekering van HCl biedt geen dekking voor individuele praktijken.

Een eventuele cyberverzekering van HCl is uitsluitend bedoeld voor de eigen organisatie en de risico's die onder de betreffende polis vallen.

Dit betekent dat:

- De praktijk zelf verantwoordelijk is voor het beheersen van cyberrisico's binnen de eigen organisatie.
- De praktijk zelf bepaalt of het afsluiten van een cyberverzekering wenselijk is.
- Beveiligingsincidenten binnen de eigen praktijk niet automatisch onder een verzekering van HCl vallen.

Een eigen cyberverzekering kan helpen om bepaalde financiële gevolgen van een cyberincident te beperken.

Let op: Een cyberverzekering is geen vervanging voor goede beveiligingsmaatregelen, zorgvuldig gebruikersbeheer en duidelijke interne procedures.

Tot slot

Privacy en informatiebeveiliging zijn een gezamenlijke verantwoordelijkheid, met een duidelijke verdeling van taken en verplichtingen.

HCl zorgt voor passende beveiliging binnen haar dienstverlening. De praktijk blijft verantwoordelijk voor het zorgvuldig omgaan met patiëntgegevens en het naleven van de privacywetgeving binnen de eigen organisatie.

Door deze verantwoordelijkheden helder te houden en samen aandacht te besteden aan informatiebeveiliging, dragen we bij aan een veilige en betrouwbare verwerking van patiëntgegevens.