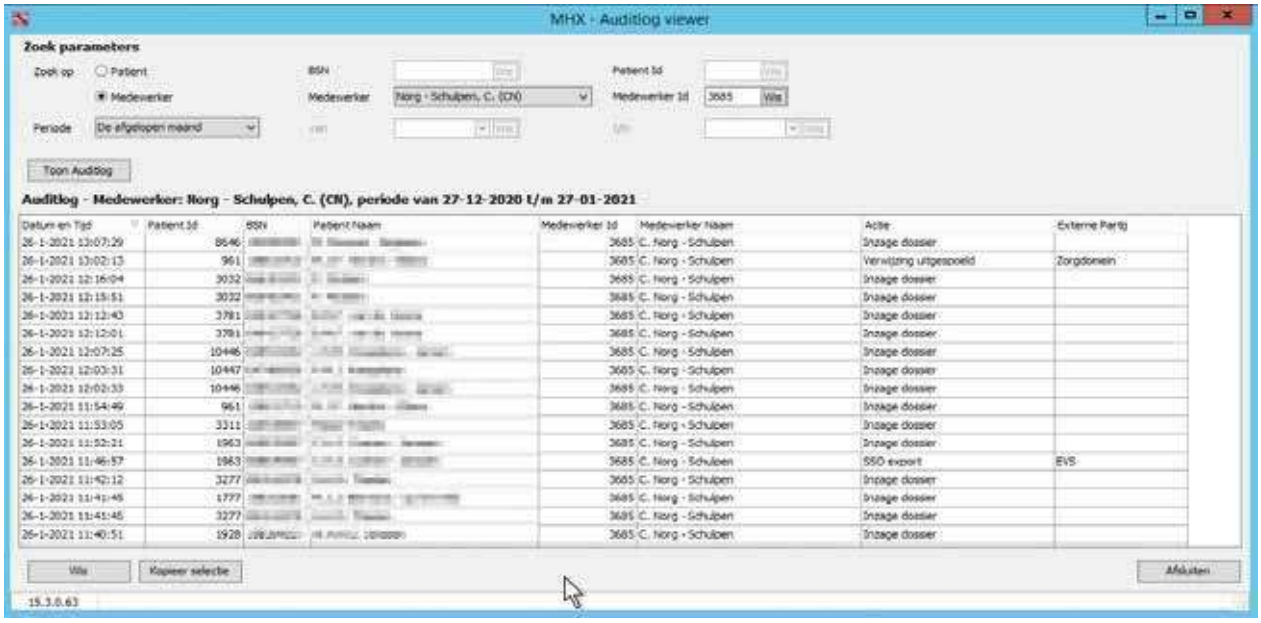
MicroHIS
Wie heeft inzage (gehad) in patiënt-gegevens?

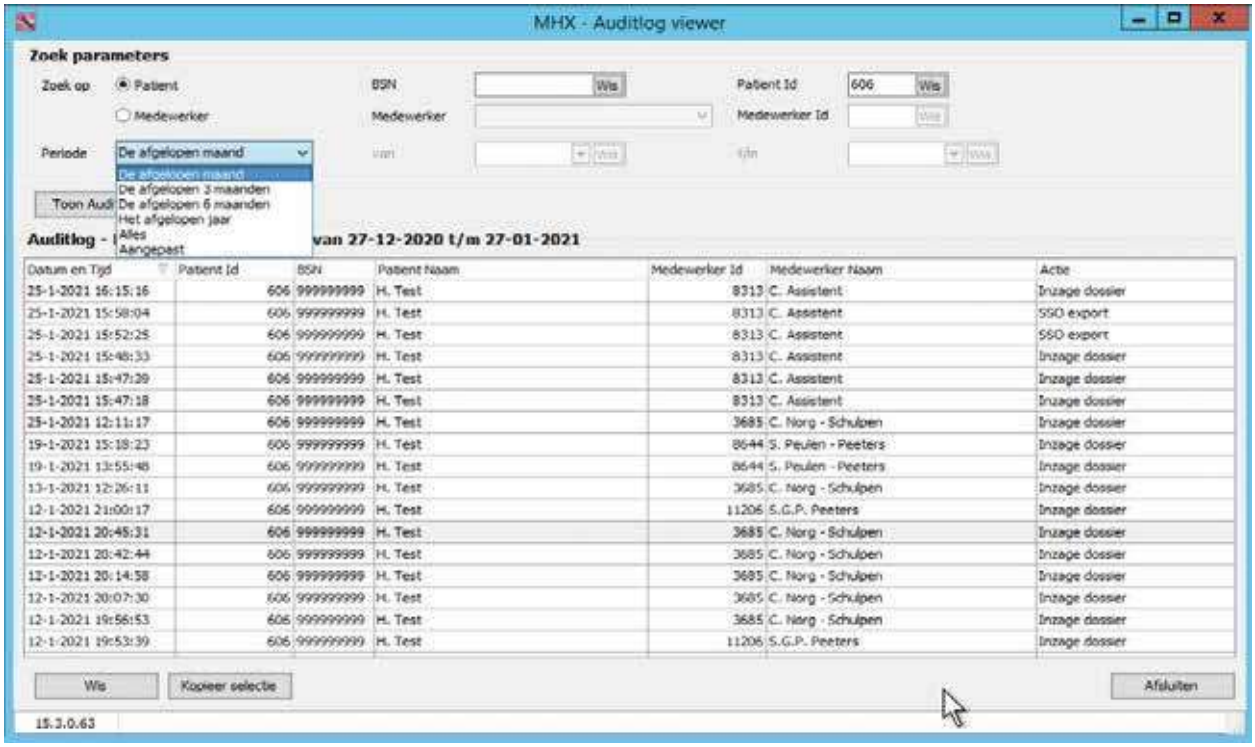
Voor het dagelijks werk van medewerkers van een huisartsenpraktijk, of dat nu de huisarts, assistente of de praktijkondersteuner is, is toegang tot de medische gegevens van de patiënten onontbeerlijk. Vrijwel altijd gebeurt inzage met de juiste reden en intentie. Toch kan raadpleging van deze gegevens ongewenst en onterecht zijn. Het bijhouden van een toegangslog maakt het mogelijk om dit ongewenste gedrag zichtbaar te maken. Regelmatige controle is wenselijk, zodat, weliswaar achteraf, maatregelen genomen kunnen worden.

In MicroHIS wordt vastgelegd wie, wanneer welk patiëntendossier raadpleegt. Om te waarborgen dat de logging overzichtelijk blijft, worden er ook heel veel zaken niet gelogd. In MicroHIS wordt *niet* gelogd:

- welk onderdeel van het patiënten dossier is bekeken;
- wie welke informatie heeft toegevoegd;
- wie welke informatie heeft gewijzigd;
- wie welke informatie heeft verwijderd



Figuur 1. Het auditlog per medewerker



Figuur 2. Het auditlog per tijdsperiode

Ook het raadplegen van werkbladgegevens vanuit de agenda wordt *niet* gelogd.

De logging is eenvoudig op te roepen. Start het programma MHXAuditLogViewer. Log in met gebruikersnaam en wachtwoord.

Kies voor zoeken op medewerker en de te raadplegen periode (default staat deze op de laatste maand). U ziet nu welke dossiers zijn geraadpleegd en van welke patiënt gegevens naar buiten zijn gestuurd, *verwijzing gemaakt* en *SSO export*. SSO staat voor *Single Sign On*, dat wil zeggen dat via een automatische inlog naar een ander programma gekoppeld wordt. Denk aan gegevens die uitgespoeld worden naar Zorgdomein, VIPlive, Ksyos, NHG-Doc, Prescriptor EVS (zie figuur 1).

Daarnaast kan een patiënt inzage verzoeken in de toegang tot zijn dossier. Hiervoor kunt u in de MHXAuditLogViewer zoeken door het HIS-nummer of het BSN van de patiënt in te voeren en de te raadplegen periode te kiezen (default staat deze op de laatste maand; zie figuur 2). Ook hier is te zien welke gegevens naar buiten zijn gegaan, waaronder ook LSP-bevraging en MEDOVD-export.

Deze data kunt u desgewenst kopieren naar het klembord via de knop **Kopieer selectie** en vervolgens in een andere toepassing plakken, bijvoorbeeld Excel of Word, en zo aan de patiënt geven.

Figuur 3. Blokkeren van de inzage via het patiëntenportaal

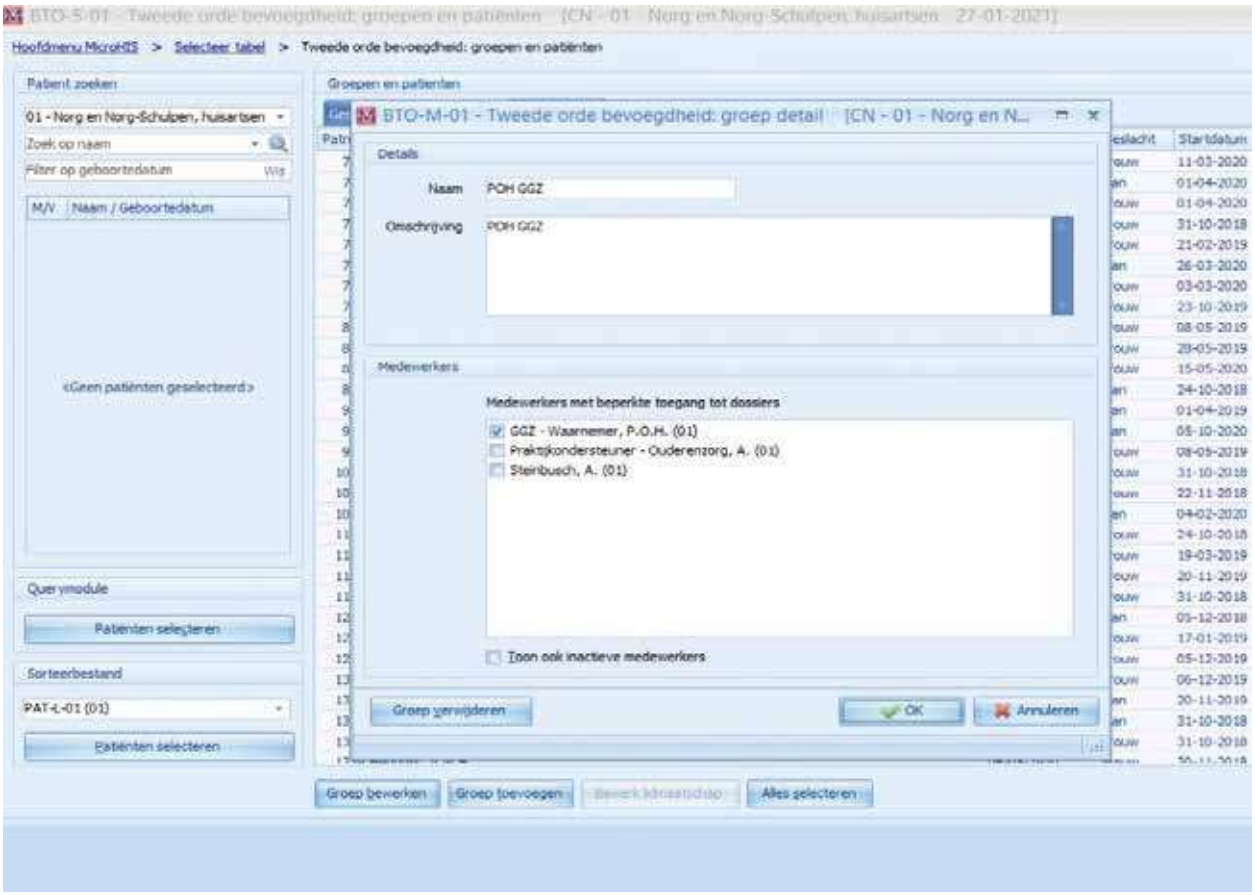
'Primaire preventie'

Zoals gezegd gaat het hier om controle achteraf, terwijl 'preventie' bestaat uit het opsporen van medewerkers die misbruik maken van hun toegang tot de gegevens, om herhaling te voorkomen.

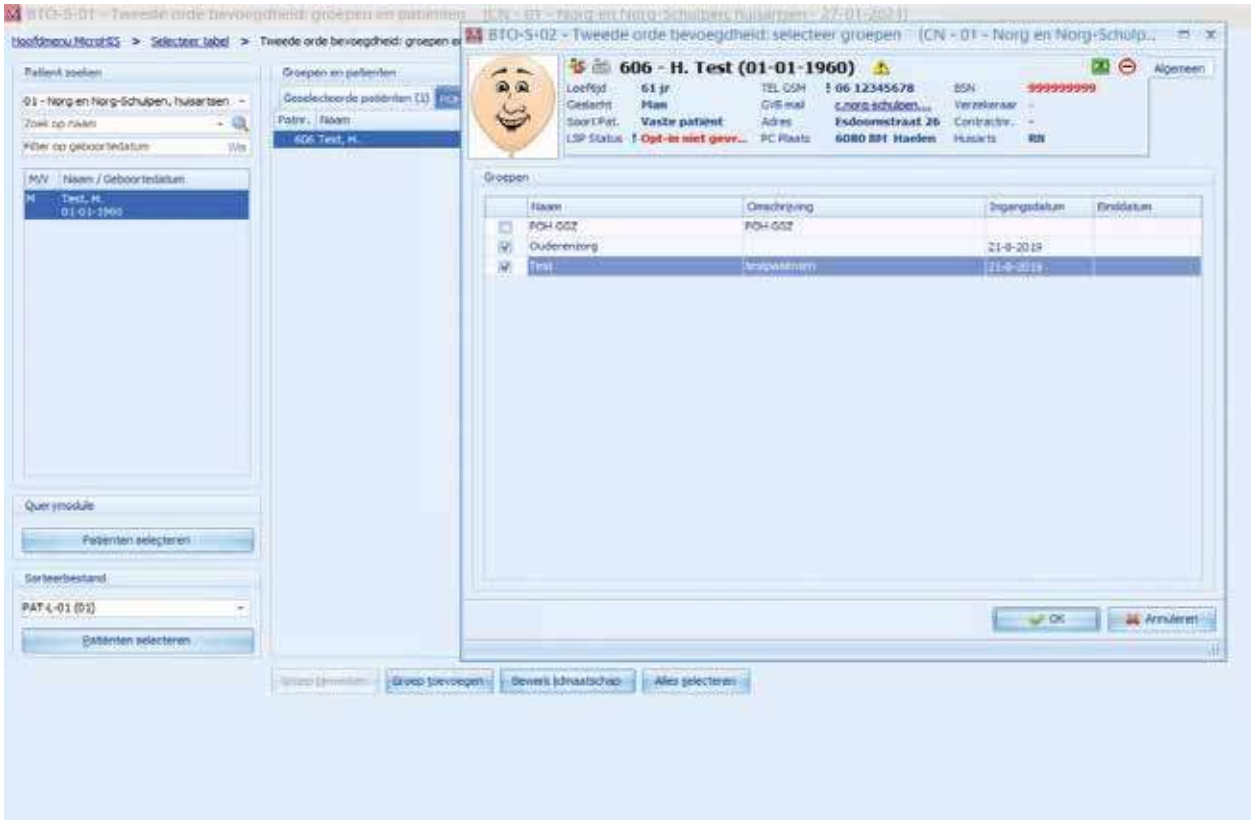
Is er dan helemaal geen 'primaire' preventie mogelijk? Jazeker.

- De patiënt wil niet dat zijn gegevens worden uitgespoeld voor het LSP: registreer bij opt-in gegevens *gevraagd*, maar geen vinkje bij *akkoord*, dus feitelijk opt-out. Er is dan ook geen toegang door de tijdelijke corona-opt-in.

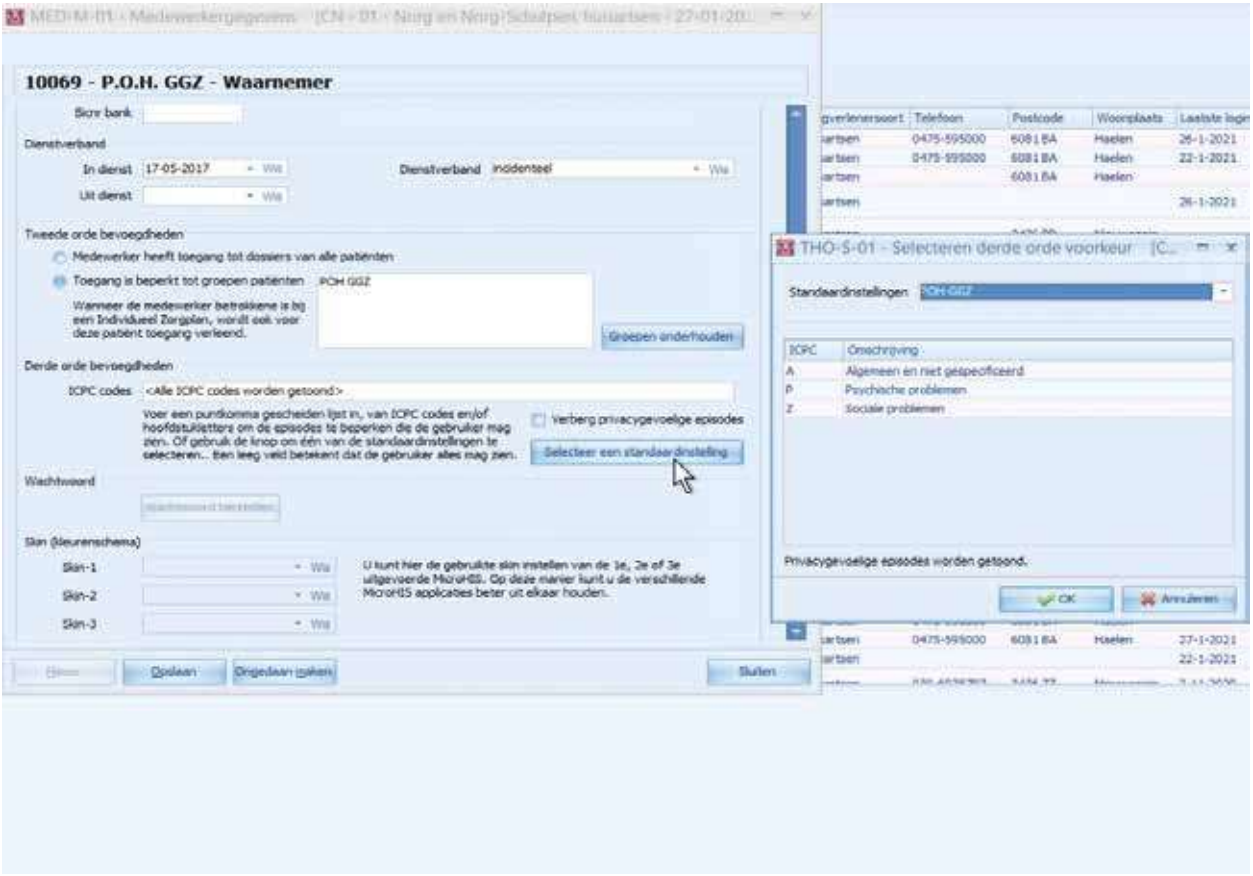
- Delen van het dossier kunt u afschermen voor bevraging van buiten door ze als privacygevoelig te markeren. Zie hiervoor de tip en truc in *SynthesHis* nummer 1 van 2020.



Figuur 4. Groepen van patiënten; de medewerker heeft alleen toegang tot deze groep



Figuur 5. Het toevoegen van een patiënt aan een groep of groepen



Figuur 6. De toegang tot bepaalde ICPC-codes beperken

- In principe kan alleen de patiënt zelf inzage krijgen via het patiëntenportaal. Maar wanneer dit (tijdelijk) toch niet wenselijk is, kunt u dit blokkeren. Ga bij patiëntgegevens naar het tabblad **Praktijk** en zet het vinkje uit bij *PS inzage van portaal of PGO* (zie figuur 3).

- Voor medewerkers kunt u de toegang tot bepaalde patiënten beperken. Via de Tweede orde bevoegdheid kunt u van patiënten groepen maken. Zo krijgt bijvoorbeeld de poh-ggz alleen toegang tot die dossiers waar hij/zij ook daadwerkelijk bemoeienis mee heeft.

Ga via systeembeheer naar **Autorisatie – Tweede orde bevoegdheid**. Hier kunt u een groep met patiënten maken, zoals te zien in figuur 4. De patiënten kunt u selecteren via een query of handmatig toevoegen. Selecteer een patiënt of query en klik op **Bewerk lidmaatschap**. Kies de groep waaraan toegevoegd moet worden (figuur 5).

- Bij de medewerkergegevens van de poh-ggz kunt u vervolgens aangeven dat deze alleen toegang heeft tot deze groep patiënten.

- De toegang tot het dossier kunt u voor bepaalde medewerkers beperken tot de regels die aan bepaalde episodes gekoppeld zijn. Deze *Derde orde bevoegdheid* is eveneens in te stellen bij de medewerkergegevens. Zoals te zien is in figuur 6 is hiervoor een aantal standaardepisodegroepen ingesteld. Maar het is ook mogelijk om hier een eigen selectie te maken.

- U kunt privacygevoelige episodes voor bepaalde medewerkers ook verbergen om onbevoegde toegang te beperken. Dit is in te stellen door een vinkje te plaatsen bij de medewerkergegevens, ook zichtbaar in figuur 6.

CAROLINE NORG-SCHULPEN
PRAKTIJK.NORG@HOME.NL

Kijk voor meer Tips en trucs op Haweb in de groep Orego (alleen voor leden) verenigingszaken.