

Chez le médecin généraliste

(1) Sélection des données TDS et le NISS des patients dans le DMI du médecin (l'émetteur de données TDS)

ENCRYPTAGE 1 des données, mais pas le NISS (par Module Encryptage ou Messagerie*, indépendant du logiciel healthdata.be)

(2) Envoi de message crypté avec des données cryptées + NISS des patients vers la plateforme eHealth

ENCRYPTAGE 2 du message (par Module Encryptage ou Messagerie*, indépendant du logiciel healthdata.be)

Plateforme eHealth

(3) Décryptage du message contenant le NISS et les données qui restent cryptées. **CODAGE 1 = Pseudonymisation du NISS par un algorithme (conçu sous la supervision du Comité Sectoriel Santé)**

PAS de stockage.

(4) Envoi de message crypté avec données cryptées et pseudoNISS vers Healthdata.be

ENCRYPTAGE 3 du message

Chez [Healthdata.be](https://healthdata.be)

(5) Décryptage des données cryptées +

CODAGE 2 = double chiffrement du pseudoNISS par Healthdata.be

(6) Analyse des données pseudonymisées dans le cadre de l'étude scientifique, par les chercheurs, mais pas par Healthdata.be

(7) Contrôle (log) en continu des accès aux données et des actions effectuées par les chercheurs

*différentes configurations ont été mises en place par les services TIC/DMI.