

23 Système d'Information du Réseau FranceCoag : une architecture pour la télétransmission sécurisée de données médicales

M. Ghez¹, D. Soulier¹, T. Calvez²

¹InVS, Saint-Maurice – ²Inserm EMI 0214, Paris

Contexte

Le Réseau FranceCoag est un projet coordonné par l'Institut de veille sanitaire depuis le 1^{er} janvier 2004 dont les objectifs sont les suivants :

- connaître de façon exhaustive la répartition géographique, les caractéristiques et l'évolution de la population atteinte de **maladies hémorragiques dues à des déficits héréditaires en protéines coagulantes** prise en charge dans les centres de traitements spécialisés ;
- disposer d'un outil de veille sanitaire permettant l'investigation de toute suspicion de transmission par des préparations de facteurs de coagulation d'un **agent transmissible** nouvellement identifiable ;
- mieux connaître les facteurs de risque d'inhibiteur chez les enfants atteints d'une hémophilie sévère et les modalités de prise en charge des inhibiteurs chez ces patients ;
- évaluer la faisabilité, l'observance, la tolérance et l'impact de traitements prophylactiques standardisés chez les enfants atteints d'une hémophilie sévère.

Pour répondre à ces objectifs, une **cohorte prospective multicentrique** a été constituée. Les partenaires du Réseau sont les personnels des centres de traitements spécialisés (36 CTS en France métropolitaine et DOM). Le Centre coordinateur (CC) est intégré au Département des maladies chroniques et traumatismes.

Circuit de l'information

Lors de chaque visite de suivi dans la Cohorte FranceCoag, un formulaire est complété. La transition entre formulaires papier et formulaires électroniques est en cours. Depuis juin 2004, quelques données de base (identifiant du patient, date de la visite, date de la visite précédente) sont télétransmises le jour même de la visite (figure 1). Le formulaire est ensuite complété et envoyé au CC dans le mois qui suit la visite.

Caractéristiques des données transmises

Des données de santé à caractère personnel sont transmises dans le Réseau. L'identification des patients s'appuie sur un numéro d'anonymat attribué dans les CTS et conservé localement dans une liste de correspondance. Néanmoins d'autres données sont identifiantes (telle la date de naissance) ce qui impose la mise en place de garanties de confidentialité spécifiques.

Application de saisie à distance

Les différents formulaires de cette étude sont implémentés sous forme de formulaires web (en utilisant des logiciels libres : Apache, PHP, PostgreSQL). Les données sont saisies dans les centres en utilisant un navigateur web standard. Les données saisies sont soumises à des contrôles de cohérence et de validité avant d'être stockées.

Le CC peut demander aux médecins partenaires de faire des corrections sur les formulaires saisis. Une fois ceux-ci définitivement validés, ils sont transférés dans une base uniquement accessible par le CC.

Figure 1 - Formulaire de signalement

The screenshot shows a web browser window with the URL <https://www.francecoag.org/restricted/?page=signalement&action=new&cohort=francecoag>. The page title is 'Signaler une visite'. The form includes the following fields:

- Centre:
- Num. patient:
- Date de la visite:
- Date de la dernière visite:
- Année de naissance du patient:
- Centre précédent:
- Numéro précédent:
- Nom du clinicien ayant réalisé la visite:
- Prélèvements envoyés à la bibliothèque: oui non biothequ
- Inclusion dans le Réseau FranceCoag: oui non inclusion
- Patient décédé: oui non deces
- Statut:

Buttons: 'Envoyer le formulaire' and 'Fermer la session'.

Architecture de sécurité

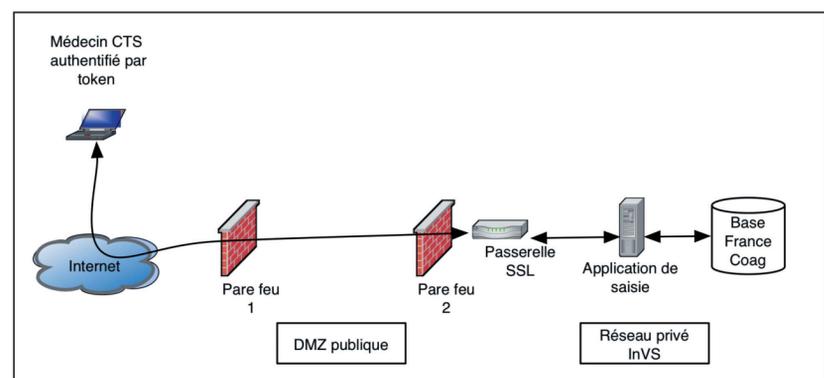
Réseau privé virtuel (RPV)

Par mesure de sécurité, les serveurs hébergeant l'application de saisie des formulaires sont situés dans un sous-réseau spécifique du réseau local de l'InVS. Ils ne sont pas accessibles directement par un attaquant extérieur. Les médecins partenaires accèdent à l'application à travers un tunnel sécurisé (chiffrement SSL) créé entre le réseau du centre et le réseau de l'InVS et passant par Internet.

Authentification des utilisateurs

Les médecins partenaires ayant accès à des ressources sensibles, il est nécessaire de recourir à des moyens d'authentification forte de ces utilisateurs. Une solution d'authentification à 2 facteurs a été retenue (type token ou carte à puce).

Figure 2 - Architecture de télétransmission



Perspectives

Ces technologies de télétransmission sécurisées sont encore en expérimentation et devraient être déployées plus largement à l'InVS pendant l'année 2005. Chaque projet fait l'objet d'une demande d'autorisation préalable à la Cnil.

Pour plus d'informations : <http://www.francecoag.org>