

Garanties apportées par le DCC pour le secret médical.

1. Conformité CNIL

Le réseau Oncopl a reçu l'autorisation CNIL, faisant référence à la délibération n°2005-025 portant autorisation (dossier n°1050555) de mise en œuvre par l'association Onco Pays de la Loire d'un dossier médical partagé. SANTEOS est l'hébergeur de l'application DCC. Les systèmes d'information SANTEOS bénéficient d'un récépissé de déclaration à la CNIL (N° 727983) pour l'ensemble de ses services (dont dossier médical partagé et télé-expertise) et répondent ainsi aux règles en vigueur concernant la sécurité et la confidentialité des données médicales.

Le site d'hébergement de SANTEOS, ses infrastructures réseaux et ses systèmes ont été audités entre 2005 et 2007, par un cabinet indépendant qui n'a révélé aucune faille de sécurité.

Consentement du patient

Le médecin responsable de la prise en charge du patient lui fait signer son consentement pour la création et l'alimentation de son DCC ainsi que pour l'habilitation de l'équipe médicale responsable de sa prise en charge, à partir des documents ci-joints, validés par les instance Oncopl.

2. Identification des PS¹ sur le portail DCC

Le professionnel de santé peut s'identifier de 2 façons :

- Soit par un couple « identifiant + mot de passe ». Le mot de passe est attribué par un algorithme propriétaire, il est non significatif et supérieur à 7 caractères alphanumériques.
- Soit le Professionnel de Santé s'identifie grâce à sa carte CPS ; le Professionnel de Santé introduit sa carte dans le lecteur et saisit son code personnel. C'est le moyen d'identification privilégié en regard du décret confidentialité du 15 mai 2007.

3. Accès au dossier patient

Par défaut les PS ne peuvent pas voir le contenu des dossiers patients. Seul le PS ayant créé le DCC peut accéder à son contenu. Ce médecin « agréé » peut ensuite habilitier un confrère ou une équipe médicale pour lui permettre l'accès au DCC du patient. Cette habilitation est conditionnée à l'obtention du consentement signé du patient.

4. Protocoles de sécurisation des échanges

Le serveur Web du DCC met en œuvre le protocole de sécurité SSL à clé publique forte.

A chaque session entre un navigateur et le serveur une nouvelle clé est générée aléatoirement. Les versions récentes des navigateurs assurent un cryptage fort à 128 bits.

Le protocole SSL présente les avantages suivants :

- le client authentifie le serveur grâce au certificat serveur,
- les données échangées sont cryptées, ce qui garantit la confidentialité. Le système de clé publique et clé privée permet d'assurer à l'émetteur de l'information que seul son correspondant pourra lire le message.
- un contrôle d'intégrité vérifie que les données échangées entre le client et le serveur n'ont pas été modifiées durant le transfert. Le message crypté qui part de l'ordinateur du Professionnel de Santé vers le site SANTEOS ainsi que les informations émises par le serveur Web parviennent intacts à leur destinataire.

5. Journalisation des événements

Tous les événements DCC (connexion, déconnexion, accès, lecture, modification,...) sont enregistrés dans les journaux systèmes du DCC. Si besoin est, il est possible de remonter dans le temps pour tracer un événement autour d'un patient et d'un PS donnés.

¹ Professionnel de Santé