

EVOLUTION DES MODES D'AUTHENTIFICATION AU DCC ONCOPL



Afin de se conformer aux obligations réglementaires, les modes d'authentification au DCC ONCOPL évoluent !



Pourquoi renforcer l'authentification au DCC ?



Le Dossier Communicant de Cancérologie (DCC) contient des informations sensibles concernant les patients et leur prise en charge.



Que pourrait entraîner un accès non sécurisé ?

- Des fuites de données
- Des utilisations malveillantes ou des atteintes à la confidentialité des données patients



L'objectif ?

- Se conformer à la réglementation en vigueur
- Protéger les utilisateurs
- Assurer une meilleure fiabilité du système

Se connecter au DCC aujourd'hui



Qu'existe-t-il ?

- 1- Login/mot de passe
- 2- **Pro Santé Connect (PSC)** : Permet une connexion sécurisée via une carte CPS ou une e-CPS.
- 3- **Appel contextuel** : Pour les établissements disposant d'un interfaçage entre leur DPI et le DCC.

Authentification à double facteur



En quoi consiste-t-elle

A réduire considérablement les risques liés aux compromissions de mots de passe et à vérifier l'identité de l'utilisateur en deux étapes, comme suit :

- 1- Saisir l'identifiant et le mot de passe
- 2- Saisir le code temporaire reçu via une application mobile (TOTP) ou par e-mail (OTP)



Se connecter au DCC à partir du 26/03/25



De quelle façon ?

- 1- **Pro Santé Connect (PSC)** : Recommandé par l'ANS¹, permet une connexion sécurisée via une carte CPS ou une e-CPS.
- 2- **Appel contextuel** : Pour les établissements disposant d'un interfaçage entre leur DPI et le DCC.
- 3- **Application TOTP²** : Codes temporaires générés par une application tierce.³
- 4- **OTP par e-mail** : Code unique reçu sur l'adresse mail rattachée au compte utilisateur.

Liens utiles :



En savoir + sur la CPS et commander votre carte



Utilisation du DCC et FAQ "Me connecter au DCC via Pro Santé Connect"



1. Agence du Numérique en Santé
2. Time-based One-Time Password

3. Exemples d'applications recommandées :

Google Authenticator (Android et iOS), Microsoft Authenticator (Android et iOS), Authy (Android, iOS et Desktop), FreeOTP (open source, Android et iOS...)

