

INFOBRIEF

HospiConnect : Offrir un accès sécurisé mais facile aux systèmes nationaux de santé

Comment Imprivata contribue à la sécurité et à l'efficacité des flux cliniques pour HospiConnect

Le 7 janvier 2026, le ministère de la Santé a publié le calendrier de la deuxième partie du programme Hop'En, baptisée Hop'En 2. Cette nouvelle initiative s'inscrit dans la continuité des programmes CaRE et Hop'En pour la période 2023-2027. Elle met l'accent sur l'identité numérique, la sécurité d'accès et la capacité à utiliser efficacement les services nationaux tels que le DMP.

HospiConnect marque une évolution majeure vers la généralisation de l'authentification forte et de l'accès nominatif aux systèmes critiques de santé.

La plateforme Imprivata combine authentification forte (MFA) et accès rapide aux applications grâce au SSO, permettant de renforcer la sécurité sans multiplier les contraintes pour les utilisateurs.

Calendrier :



 **2026** – Mise en œuvre et structuration

 **2026 – 2028** : Calendrier pour atteindre l'objectif Hopen'2/Hospiconnect

DATES CLÉS

Cette année est cruciale pour intégrer le programme et obtenir un financement futur.

13 février 2026 – Date limite de dépôt des candidatures pour les hôpitaux souhaitant participer au programme HospiConnect / HOP'EN 2.

Toutes les preuves d'investissement (Imprivata pour SSO, gouvernance des identités, services) doivent être soumises au mois de juin chaque année (2026 – 2027 – 2028). Source: [Bulletin officiel du 12 Janvier 2026](#)

Pourquoi cela vous concerne ?

LE RISQUE CYBER EN QUELQUES CHIFFRES

3^{ème} secteur

le plus touché. Les établissements publics de santé représentent 10% des attaques par rançongiciel (ANSSI).

+ 10 %

d'attaques par rançongiciel en 2023 visant le secteur de la santé (CERT Santé).

1 173

déclarations d'incidents en 2023 et 2022 (CERT Santé).

Source: [Cybersécurité accélération et Résilience des Etablissements \(CaRE\)](#)

Renforcer la sécurité des accès ne doit pas se faire au détriment de la fluidité des parcours de soins et perturber la prise en charge des patients. Dans les environnements cliniques, où les professionnels de santé se déplacent constamment et partagent les postes de travail, la sécurisation des accès doit s'intégrer naturellement aux pratiques de soins.

La gestion des identités et des accès dans le système national de santé évolue

Dans le cadre d'HospitConnect, les établissements de santé doivent adopter une gestion des identités et des accès qui comprend des méthodes d'authentification renforcées (SSO) avec des cartes (CPSvx). Ces exigences découlent de la conformité au RGPD et de la mise en œuvre de la nouvelle directive européenne NIS2, qui impose une cybersécurité renforcée dans les secteurs critiques et essentiels tels que la santé. En outre, il existe une volonté d'unifier les systèmes d'identification actuellement utilisés dans les différents établissements d'un GHT (Groupement Hospitalier Territorial).

Ces mesures visent à réduire les cyber-risques et à améliorer la confidentialité des patients. Il est essentiel qu'elles soient mises en œuvre sans compromettre la continuité des soins.

Exemple pratique :

Un professionnel de santé qui accède à différentes applications sur plusieurs postes de travail/appareils partagés pendant son service peut rencontrer les problèmes suivants :

- Augmentation significative du nombre de connexions/déconnexions
- Des centaines de clics supplémentaires par service
- Augmentation de la charge cognitive et perturbation du flux de travail

Sans optimisation des flux de travail cliniques, cela peut entraîner :

- Des retards dans l'accès aux systèmes de soins intensifs
- Un risque accru de déconnexions incomplètes (risque pour la sécurité)
- Des solutions de contournement telles que des cartes à puce laissées dans les lecteurs ou des mots de passe notés sur papier pour partager les identifiants

Pourquoi une solution dédiée au secteur de la santé ?

Lorsqu'elles développent des processus pour répondre aux exigences HospiConnect, les organisations de soins de santé doivent installer des solutions qui combinent une authentification forte et une facilité d'utilisation pour des flux cliniques plus fluides.

Cela ne fonctionne tout simplement pas dans un environnement de soins de santé pour les raisons suivantes :

- Chaque professionnel de santé doit se connecter sur chaque appareil qu'il utilise.
- Il n'y a pas de changement rapide d'utilisateur pendant les services ou lors des changements d'équipes.
- La session ne se déconnecte pas automatiquement lorsque le personnel de santé est appelé dans un autre service.
- Cela dépend des smartphones personnels ou d'équipements spécifiques.
- Cela augmente les frais généraux de fonctionnement des établissements de santé.

Quelles sont les exigences du programme HospiConnect et comment Imprivata peut-il vous aider dans ce projet ?

HospiConnect marque une évolution majeure vers la généralisation de l'authentification forte et de l'accès nominatif aux systèmes critiques de santé : le SSO sécurisé clinique.

Les exigences	Comment Imprivata vous accompagne
Maîtriser la chaîne de gestion des identités et des accès au SIH et permettre la consultation du DMP	Imprivata sécurise et fluidifie les accès au SIH grâce à une authentification nominative, un accès contextuel via SSO et une authentification forte (MFA), garantissant traçabilité et conformité réglementaire, y compris pour l'accès au DMP.
1.1 – Gestion des identités : l'identifiant RPPS des utilisateurs est connu du DPI	Imprivata EAM garantit un accès nominatif aux systèmes et au DPI en s'appuyant sur l'identité professionnelle (RPPS), assurant une traçabilité conforme des accès.
1.2 – Gestion des Habilitations : les permissions d'accès au DPI sont mises à jour lors des mouvements de personnel	Imprivata s'interconnecte via API aux référentiels d'identités afin d'appliquer automatiquement les droits d'accès définis et de prendre en compte les évolutions liées aux mouvements de personnel.
1.3 – Utilisation d'un Moyen d'identification électronique Double facteurs 2FA pour l'accès au DPI (conformité Référentiel d'Identification Electronique)	Imprivata combine SSO et authentification forte (MFA) pour sécuriser l'accès au DPI, en prenant en charge les moyens d'identification conformes aux exigences réglementaires.
1.4 – Accès possible des utilisateurs du DPI au DMP en mode intégré : ES homologué AIR simplifié (ou API PSC)	Imprivata facilite un accès fluide et sécurisé au DMP depuis le DPI grâce au SSO clinique sécurisé, tout en garantissant une authentification conforme et une traçabilité des accès.

Présentation de la plateforme Imprivata pour l'accès aux systèmes nationaux de santé

Imprivata fournit des solutions de gestion des accès spécialement conçues pour répondre aux exigences spécifiques des flux de travail dans le secteur de la santé. Imprivata EAM (Enterprise Access Management) offre une authentification rapide et sécurisée aux services fournis par les organismes de santé nationaux, conformément aux exigences réglementaires et de sécurité, tout en garantissant un accès rapide et fluide aux systèmes critiques. Il offre une authentification unique (SSO) aux établissements de santé pour leur permettre d'accéder en toute sécurité aux services nationaux, tout en fournissant des flux de travail efficaces adaptés aux cliniciens.

PRINCIPALES FONCTIONNALITÉS :



1. Intégration avec les systèmes nationaux d'identification

Imprivata EAM s'intègre aux systèmes d'identification nationaux afin de fournir une authentification conforme aux normes EHR, tout en garantissant une expérience fluide et sécurisée aux professionnels de santé.



2. Authentification et SSO pour toutes les applications

Grâce à Imprivata pour l'authentification unique (Single Sign-On), les professionnels de santé peuvent accéder de manière sécurisée et automatique à toutes les applications cliniques et commerciales sans avoir à saisir à nouveau leurs mots de passe ni interrompre leurs flux de travail.



3. Authentification multifactorielle forte - MFA

Imprivata prend en charge plusieurs méthodes d'authentification forte (notamment les cartes professionnelles, les badges de proximité, CPS, FIDO2, MIFARE DESFire, la biométrie, OTP, OIDC et SAML) afin de sécuriser l'accès en fonction des utilisations cliniques et des exigences EHR.



4. Interopérabilité clinique : postes de travail partagés et environnements multi-utilisateurs

Imprivata sécurise les postes de travail partagés et les bornes interactives dans les environnements cliniques, permettant une identification rapide et automatique des utilisateurs en fonction de leur profil, sans compromettre la confidentialité ou la continuité des soins.



5. Sécurité renforcée, transparente pour les professionnels de santé

Imprivata réduit la dépendance aux mots de passe grâce à des mécanismes d'authentification intelligents, alliant haute sécurité, facilité d'utilisation et gain de temps pour les équipes de santé.



6. Adapté aux organisations multi-sites (GHT)

Imprivata permet une gestion centralisée des identités et des accès au sein des GHT, avec des politiques de sécurité cohérentes, un référentiel unique et une gouvernance simplifiée entre les entités.





Avantages pour les professionnels de santé

- Accès rapide et familier grâce à une authentification simple par carte (« tap & go ») pour tous les services et départements, ainsi que sur tous les terminaux et appareils médicaux.
- Aucune dépendance à un seul appareil.
- Réduit la fatigue numérique liée à la connexion et à la déconnexion.
- Flux de travail cliniques partagés plus sûrs et plus sécurisés, avec fermeture automatique des sessions.
- Jusqu'à 45 minutes gagnées par clinicien sur chaque service, qui peuvent être consacrées aux soins des patients.

Avantages pour les équipes informatiques et de sécurité

- Adoption rapide : pas besoin de repenser les flux de travail
- Fonctionne sur différents appareils partagés, postes de travail et zones cliniques
- Rapports centralisés pour l'accès, la sécurité, l'audit et la conformité.
- Gestion centralisée des identités et des accès dans l'ensemble du groupe hospitalier.



Conclusion

À l'approche de 2026, la directive européenne NIS2 et le programme HOP'EN 2 – HospiConnect redéfinissent les standards de sécurité et de gestion des accès au sein des établissements de santé. Cette évolution ne relève plus uniquement de la conformité : elle marque une transformation durable des systèmes d'information, où l'identification fiable des professionnels et la protection des accès deviennent des prérequis du fonctionnement hospitalier.

Dans des environnements caractérisés par la mobilité des équipes, les postes partagés et la nécessité d'accéder rapidement à l'information, le défi consiste désormais à renforcer la sécurité sans alourdir les pratiques de soins. Car dans le secteur de la santé, chaque seconde compte ! Et la meilleure sécurité est souvent celle qui sait se rendre invisible.

En combinant authentification forte et accès rapide aux applications grâce au Single Sign-On (SSO clinique sécurisé), Imprivata accompagne les établissements dans leur trajectoire HospiConnect en conciliant exigences réglementaires, efficacité opérationnelle et simplicité d'usage. Anticiper ces évolutions dès aujourd'hui, c'est se donner les moyens de répondre aux nouvelles obligations tout en construisant un modèle d'accès sécurisé, fluide et durable.

Car demain, la capacité des organisations de santé à protéger l'accès à l'information sera indissociable de leur aptitude à le rendre simple, rapide et toujours au service du soin.

PRENEZ RENDEZ-VOUS AVEC L'UN DE NOS EXPERTS



Imprivata est un éditeur de logiciels spécialisé dans l'identité numérique, l'authentification et la gestion des accès pour les organisations des secteurs critiques. L'entreprise redéfinit la manière dont ces organisations résolvent les défis complexes liés aux workflows, à la sécurité et à la conformité, grâce à des solutions qui protègent les données et applications critiques sans perturber les flux de travail. Sa plateforme de solutions interopérables de gestion de l'identité, d'authentification et d'accès permet à des organisations, dans plus de 45 pays, de gérer et de sécuriser entièrement toutes les identités numériques — internes comme tierces — en établissant la confiance entre les personnes, la technologie et l'information.

Pour plus d'informations, veuillez nous contacter au :

Siège social mondial aux États Unis
Waltham, MA
Tél. : +1 877 663 7446
www.imprivata.com

Siège social européen
Uxbridge, Royaume Uni
Tél. : +44 (0) 208 744 6500
www.imprivata.com/uk

France
Tél. : +33 (0) 1 84 88 00 15
Email: contactfrance@imprivata.com
www.imprivata.com/fr

Allemagne
Langenfeld
Tél. : +49 (0) 2173 99 385 0
www.imprivata.com/de

Copyright © 2026 Imprivata, Inc. Tous droits réservés. Imprivata est une marque déposée d'Imprivata, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques déposées appartiennent à leurs détenteurs respectifs.

3945-2026_HospiConnect infobrief