

Comptes génériques dans les hôpitaux

la faille silencieuse qu'il faut combler

Trois idées clés concernant :

- La faille silencieuse des comptes génériques dans les hôpitaux
- HelloID : délégation directe et traçabilité totale pour les cadres
- Les bénéfices face aux exigences HAS, ANSSI et RGPD

TOOLS4EVER



Sommaire

Introduction 2

Contexte & Enjeux 3

- Qu'est ce qu'un compte générique 3
- Trois symptômes, trois risques majeurs 4

Le Paysage des menaces 5

- Les comptes génériques : vecteur d'attaque 5
- Le cadre réglementaire 5

La solution HelloID 6

- Délégation directe Vs workflow classique 6
- Le workflow en 5 étapes 6
- Fonctionnalités clés 7

Bénéfices mesurables 8

- Bénéfices par interlocuteur 8

Synthèse & prochaines étapes 9

A propos de Tools4ever 10

Introduction

Les établissements de santé font face à une double pression : une menace cyber en forte progression et des exigences réglementaires qui se durcissent. Au cœur de cette tension : les comptes génériques partagés.

Ces comptes non nominatifs constituent la principale faille identifiée lors des audits de cybersécurité hospitaliers. Impossibles à tracer, difficiles à révoquer, ils exposent les établissements à des risques majeurs : violations RGPD, non-conformité HAS, incidents ANSSI.

Ce livre blanc présente d'abord les risques liés aux comptes génériques, puis comment HelloID de Tools4ever transforme ce risque en conformité démontrée grâce à une interface de délégation directe aux cadres d'astreinte.

Ce livre blanc couvre :

- Le risque systémique des comptes génériques hospitaliers
- Le cadre réglementaire HAS Cycle 6, ANSSI, RGPD
- La solution HelloID : délégation directe et pool sécurisé
- Les bénéfices mesurables et les prochaines étapes



Contexte & enjeux

Les établissements de santé sont confrontés à une double pression : une menace cyber en forte progression et des exigences réglementaires qui se durcissent.

Les comptes génériques partagés constituent une faille structurelle majeure.

750
cyber-incidents hôpitaux 2024 (+29% ANS)

30
hôpitaux français victimes de ransomware

11,4%
des incidents ANSSI concernent le secteur santé

500k€+
coût moyen d'un incident cyber majeur en santé

**Sources : Observatoire ANS 2024, ANSSI Panorama menace santé 2024*

Qu'est-ce qu'un compte générique ?

Un compte générique est un identifiant non nominatif partagé entre plusieurs personnes.
On les rencontre systématiquement dans les services hospitaliers :

- Compte «urgences» ou «radio» partagé entre toute une équipe
- Identifiant « admin » partagé entre plusieurs techniciens IT
- Compte DPI/SIH sans responsable identifié
- Accès intérimaire jamais révoqué après la fin de mission

*Dans la **quasi-totalité des établissements** audités, les **comptes génériques** constituent la principale **faille** identifiée et la plus difficile à défendre face à un auditeur HAS ou à l'ANSSI.*

Trois symptômes, trois risques majeurs

RISQUES	IMPACT	RÉFÉRENTIEL
Comptes partagés non tracés	Impossible d'identifier qui a accédé aux données patients. L'établissement ne peut répondre à l'ANSSI ni à la CNIL en cas d'incident.	HAS 3.6-06 / ANSSI / RGPD
Comptes actifs après départ	D'anciens salariés, intérimaires ou stagiaires conservent des accès au SIH et aux DPI après leur départ.	HAS 3.6-02 Départs
Absence de workflow	N'importe quel agent peut utiliser un compte générique sans validation. Aucune traçabilité de l'attribution ni de la durée d'accès.	HAS 3.6-06 Audit SI

Le paysage des menaces

Le secteur de la santé est aujourd'hui le 3e secteur le plus ciblé par les cyberattaques.
Les hôpitaux cumulent trois facteurs d'attractivité :

Données ultra-sensibles	Continuité non négociable	SI historiquement peu sécurisé
Les dossiers patients se revendent à prix d'or sur le darknet.	Un hôpital ne peut pas s'arrêter. Cette contrainte force à payer les rançons.	Numérisation récente, budgets cyber limités, pratiques artisanales.

Les comptes génériques : vecteur d'attaque

Mouvement latéral : Un attaquant accède à toutes les ressources associés sans déclencher d'alerte, car l'usage semble «normal».

Comptes orphelins : Un ancien prestataire dont le compte n'a pas été révoqué conserve des accès au SIH indéfiniment.

Non-répudiation impossible : En cas de fuite de données via un compte générique, l'établissement ne peut identifier le responsable.

La certification HAS Cycle 6 (dès septembre 2025) intègre 21 critères impératifs sur le numérique. La non-conformité peut entraîner une certification conditionnelle ou un refus rendu public Qualiscope.

Le cadre réglementaire : des obligations précises

RÉFÉRENTIEL	EXIGENCE	IMPACT
HAS 3.6-06	Identification nominative de chaque professionnel.	Utilisation des comptes génériques non tracée = non conformité
HAS 3.6-02	D'anciens salariés, intérimaires ou stagiaires conservent des accès au SIH et aux DPI après leur départ.	Comptes actifs post-départ = violation du critère
RGPD Art. 32	N'importe quel agent peut utiliser un compte générique sans validation. Aucune traçabilité de l'attribution ni de la durée d'accès.	Comptes partagés = incapacité à démontrer la maîtrise

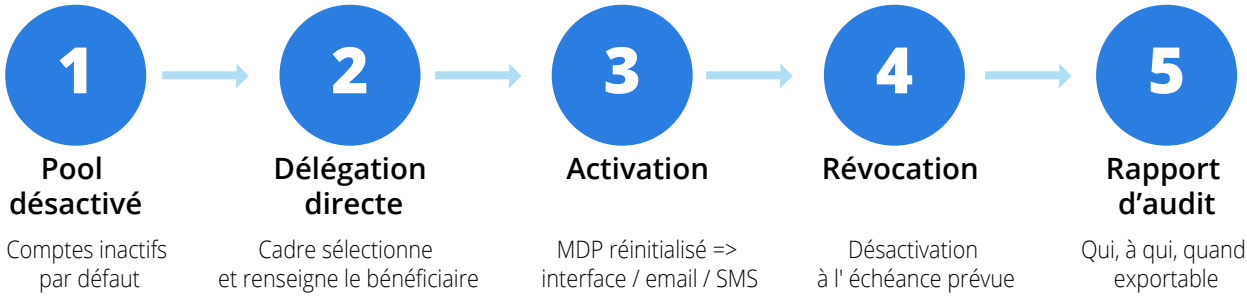
La solution HelloID

HelloID de Tools4ever propose une interface de délégation directe confiée aux cadres d'astreinte permettant un contrôle immédiat et traçable, sans latence, sans intervention de l'équipe IT.

Délégation directe vs workflow classique

	Workflow classique	Délégation HelloID
Qui agit ?	Agent demande => responsable approuve	Le cadre d'astreinte agit directement
Délai	Délai d'approbation variable	Instantané - critique la nuit et le week-end
Usage typique	Onboarding, droits permanents	Urgences, astreintes, intérimaires
Traçabilité	Journal de workflow	Délégation nominative + journal d'audit complet

Le workflow en 5 étapes



Transmission des credentials - options configurables :

- Affichage direct dans l'interface de délégation
- Envoi automatique par email au cadre et/ou au bénéficiaire
- Envoi automatique par SMS pour une transmission instantanée

Une durée maximale configurable garantit qu'aucun compte ne restera actif indéfiniment.

Fonctionnalités clés HelloID

FONCTIONNALITÉ	BÉNÉFICE CONCRET
Interface de délégation cadre d'astreinte	Accès autonome et immédiat au pool de comptes désactivés, sans passer par le helpdesk IT.
Pool de comptes désactivés par défaut	Aucun compte générique n'est actif sans attribution explicite. Zéro compte orphelin par construction.
Activation avec date de fin forcée	Durée d'accès bornée, avec durée maximale configurable et alertes avant expiration.
Réinitialisation & envoi auto MDP	Chaque activation génère un nouveau mot de passe unique transmis via interface, email et/ou SMS.
Révocation automatique + retour pool	À l'échéance, le compte est désactivé et immédiatement disponible pour une nouvelle attribution.
Journal d'audit & rapports nominatifs	Qui a attribué, qui a utilisé, quand, combien de temps. Exportable pour l'auditeur HAS/ANSSI.
200+ connecteurs	AD, Entra ID, Easily, Hôpital Manager, Orbis, Cariatides, Maincare, Cpage, Hublo, PeopleNet, Silae, Foederis, etc. sur github.com/Tools4everBV.

Bénéfices mesurables

Le déploiement de HelloID produit des résultats concrets et mesurables répondant simultanément aux enjeux de cybersécurité, de conformité et d'efficacité opérationnelle.

0
comptes génériques orphelins

< 24h
délai de traitement d'une demande d'accès

100%
traçabilité des accès aux comptes génériques

- 70%
en moyenne de charge helpdesk liée aux comptes génériques

Bénéfices par interlocuteur

INTERLOCUTEUR	BÉNÉFICES CLÉS
DSI / Responsable IT	Intégration rapide (en quelques jours). Connecteurs prêts à l'emploi. Réduction de la charge IT. Journal d'audit pour ANSSI et revues HAS.
RSSI	Élimination des comptes orphelins. Traçabilité nominative. Réduction de la surface d'attaque. Tableau de bord en temps réel.
Cadre d'astreinte	Interface immédiate 24h/24, 7j/7. Activation en moins de 2 minutes. Credentials transmis par interface, email ou SMS.
Direction Qualité / HAS	Réponse directe aux critères 3.6-02 et 3.6-06 HAS 2024/2025. Production automatique d'éléments de preuve. Réduction du risque de certification conditionnelle.

Synthèse & prochaines étapes

Les comptes génériques représentent aujourd'hui l'une des failles les plus répandues et exploitées dans les systèmes d'information hospitaliers.

La convergence entre la montée des cyberattaques et le renforcement des exigences HAS crée une obligation d'agir pour protéger les patients et la continuité des soins.

HelloID de Tools4ever propose une approche unique : confier directement aux cadres d'astreinte la gestion des comptes génériques via une interface de délégation sécurisée, en temps réel et sans intervention de l'équipe IT, tout en garantissant une traçabilité complète et une révocation automatique.

HelloID se déploie en cloud sans infrastructure propre.

Le module Service Automation est opérationnel en quelques jours sur un périmètre ciblé (exemple : urgences + intérimaires).

1
Cartographier

Identifier tous les comptes génériques dans le SI

2
Prioriser

Cibler les comptes à haut risque : urgences, radiologie

3
Piloter

Déployer HelloID Service Automation

4
Étendre

Généraliser à l'ensemble de l'établissement

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Tools4ever Europe du Sud
C/ Ramon Turró 169 A
08005 Barcelone
Espagne

Site web : Tools4ever.fr
Email : seales@tools4ever.com