TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

SOLUTIONS ABORDABLES DE GESTION DES IDENTITÉS, ACCÈS ET MOTS DE PASSE POUR LE **SECTEUR HOSPITALIER**

AVEC L'INTRODUCTION DE NOUVELLES RÈGLEMENTATIONS COMME LA CARTE PROFESSIONNEL DE SANTÉ (CPS) OU ENCORE, LE DOSSIER MÉDICAL PERSONNEL (DMP), LA SÉCURITÉ DES DONNÉES EST DEVENUE UN SUJET D'INTÉRÊT PRINCIPAL DANS LES HÔPITAUX. OPTIMISER LA SÉCURITÉ EXIGE UN CONTRÔLE EFFICACE ET PRÉCIS DE TOUS LES INDIVIDUS AYANT ACCÈS À DES DONNÉES CONFIDENTIELLES TELLES QUE LE DOSSIER PATIENT.

SÉCURITÉ ET RESPECT DES RÈGLES DE CONFORMITÉ POUR LA GESTION DES UTILISATEURS

de nombreux praticiens sont impliqués dans le traitement de données relatives à la vie privée et/ou à la gestion d'informations sensibles. De ce fait, la traçabilité des actions, l'utilisation de mots de passe complexes et la mise en œuvre de procédures spécifiques pour le personnel sortant sont devenus légion courante dans les centres hospitaliers. Les comptes utilisateurs génériques tendent de plus en plus à disparaitre au profit de comptes individuels et ces changements structurels accroissent la charge de travail déjà lourde du département Informatique.
La mise en œuvre d'un système automatisé de Gestion des Identités et des Accès aidera votre organisation à rationaliser les processus d'une manière plus efficace, de réduire la charge de travail et de réduire les coûts du service informatique.

Les solutions applicatives Tool4ever sont déployées dans un grand nombre d'établissements de santé pour les projets suivants:

- Gestion des comptes utilisateurs
- Gestion des mots de passe
- Single Sign-On (SSO)
- Réinitialisation de mot de passe en libre-service (SSRPM)

GESTION DES COMPTES UTILISATEURS

la solution IAM de Tools4ever offre aux établissements de santé la possibilité d'optimiser leurs processus de gestion des comptes utilisateurs. Par exemple, automatiser la gestion des droits d'accès aux systèmes et aux applications pendant toute la durée du contrat de l'employé. Ceci est normalement obtenu grâce à:

Auto Provisioning:
IAM Auto Provisioning est capable de créer automatiquement un compte utilisateur via des connecteurs sur votre système RH. Ces connecteurs sont également disponibles pour créer des comptes dans d'autres systèmes, tels que les systèmes de gestion du dossier patient, de pharmacie, de chirurgie ou encore de radiologie. Quand un employé quitte le service, le connecteur vers le système RH lance automatiquement une procédure de désactivation de compte utilisateur afin que la personne en question n'ait plus accès à votre réseau. Vous pouvez vous référer au verso de ce dépliant pour une liste non exhaustive de connecteurs disponibles.

Access Governance (RBAC):
En utilisant Access Governance, les établissements de santé peuvent empêcher l'accès à des informations sensibles par des employés non autorisés. IAM supporte Access Governance, ainsi, les rôles organisationnels peuvent être efficacement traduits en des droits d'accès spécifiques pour l'utilisateur.

Self-Service et gestion de Workflow:
Si les employés doivent avoir accès aux ressources du réseau tels que des applications, des listes de distribution, boîtes aux lettres fonctionnelles, etc…, ils peuvent en faire la demande eux-mêmes à l'aide d'un portail libre-service. Le système créera automatiquement un workflow pour gérer les approbations requises puis la mise en service des privilèges d'accès.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

GESTION DES MOTS DE PASSE

les normes pour les meilleures pratiques suggèrent l'utilisation de mots de passe complexes. Toutefois, l'introduction de ces mots de passe provoque souvent des effets de bords tels qu'une augmentation des appels liés à la réinitialisation de mot de passe, des plaintes venant des utilisateurs finaux et des verrouillages de comptes pendant les heures de bureau. Les solutions suivantes sont disponibles pour prévenir ces effets:

Self Service Reset Password Management:
Self Service Reset Password Management (SSRPM) offre aux utilisateurs la possibilité de réinitialiser leur mot de passe sans contacter le helpdesk. En répondant à un certain nombre de questions (ou grâce à un code PIN envoyé par SMS) les utilisateurs peuvent redéfinir leur nouveau mot de passe, ou débloquer leur compte verrouillé, à tout moment, sans aucune intervention du département informatique.

Password Complexity Manager:
Les règles de complexité dans Microsoft Windows sont limitées et compliquées à utiliser. Password Complexity Manager prend en charge un large éventail de règles de complexité et fournit des instructions aux utilisateurs finaux afin de leur permettre d'être en conformité avec la politique de mot de passe requise.

Password Synchronisation Manager:
Password Synchronisation Manager (PSM) permet aux utilisateurs de synchroniser les mots de passe à travers différentes applications afin de minimiser le nombre de mots de passe que les utilisateurs doivent retenir.

SINGLE SIGN-ON

les établissements de santé suppriment les comptes utilisateurs génériques pour des raisons de respect de conformité. Cela rend les procédures de connexion plus lourdes et prend plus de temps pour les utilisateurs finaux. Ils sont tenus de se rappeler de nombreuses procédures de connexion et doivent utiliser des mots de passe très complexes pour des raisons de sécurité.
Le Single Sign-On (SSO) répond à cette évolution en permettant aux utilisateurs de ne se connecter qu'une seule fois au réseau, et de ne plus avoir ensuite à saisir leurs mots de passe pour leurs applications.

Authentification par carte CPS
La carte CPS, déjà présente dans beaucoup d'établissements de santé, peut être utilisée pour l'authentification sur le réseau. Permettant plus de sécurité, son utilisation couplée à notre solution Single Sign On permet à l'utilisateur final d'accéder à l'ensemble de son environnement de travail grâce à cette carte professionnelle.

Fast User Switching
Les procédures de connexion peuvent être encore simplifiées en combinant le Fast User Switching avec un badge utilisateur ou une carte CPS. De cette façon, les utilisateurs accèdent aux applications en insérant leur badge et se déconnectent en enlevant leur badge. Ainsi, l'ordinateur devient disponible pour l'utilisateur suivant.

Follow-Me
En complément du Fast User Switching, la fonctionnalité de Follow-Me permet aux utilisateurs qui ont ouvert des applications sur Citrix et/ou Terminal Server de poursuivre leurs travaux sur un autre ordinateur. Il en résulte un gain de temps considérable, en particulier dans le cas de personnel itinérant faisant leur ronde dans plusieurs services et ayant besoin d'accéder à leurs données via des ordinateurs différents.

CONNECTEURS PRÊTS À L'EMPLOI

La solution IAM de Tools4ever offre des connecteurs prêts à l'emploi vers diverses applications et systèmes contenant des données utilisateur pour l'ensemble de votre établissement. Des exemples sont Active Directory, Exchange, systèmes d'information hospitalière, systèmes d'accès et autres systèmes internes ou hébergés. Quelques exemples de connecteurs prêts à l'emploi:

Orbis (AGFA), McKesson, SAP, Meditech, Peoplesoft, Lawson, GE Centricity, ANSOS, SAS, Peoplesoft, InfoSys, Kronos, Remedy, Oracle Financials et bien d'autres…

Contactez votre agence Tools4ever…

ILE-DE-FRANCE: TEL. 01 42 87 74 67 – EMAIL: FRSALES.IDF@TOOLS4EVER.COM
PROVINCE: TEL. 04 78 95 37 98 – EMAIL: FRSALES@TOOLS4EVER.COM