WALLIX
TRACE, AUDIT & TRUST

NOUS PROTÉGEONS VOS DONNÉES SENSIBLES
NOUS COMPRENONS VOS MÉTIERS

SANTÉ

CONFORMITÉ / OBJETS CONNECTÉS / CLOUD COMPUTING

Les établissements de santé sont en évolution permanente. Les enjeux de la dématérialisation et la digitalisation des usages les amènent à adapter leur Système d'Information à la mobilité des utilisateurs. **Protéger les patients, c'est aussi protéger leurs informations de santé pour éviter les fuites de données, les vols, ou les coupures de services.** La protection des données personnelles est bien au cœur des évolutions des SI de santé et il est aujourd'hui nécessaire de créer une chaîne de confiance afin de garantir le bon fonctionnement du parcours de santé. Avec l'évolution des SI vers le cloud, ces risques sont démultipliés et les enjeux amplifiés pour la chaine des prestataires d'hébergement ou de services IT.

RÉGLEMENTATIONS

- **PGSSI-S / HIPPA**
- **HDS :** agrément hébergeurs de données de santé à caractère personnel (HDS). Les candidats à l'agrément de l'ASIP Santé doivent identifier les solutions de cybersécurité aptes à contribuer à leur conformité règlementaire. Si un établissement héberge lui-même ses dossiers hospitaliers, il n'a pas besoin d'obtenir un agrément HDS. En revanche, si l'établissement met son système d'hébergement au service d'autres établissements de santé, il est soumis à la procédure d'agrément. Il en est de même pour les établissements de coopération sanitaire (groupements de coopération sanitaire - GCS -, communautés hospitalières, etc.) qui mettent à disposition de leurs membres leur système d'hébergement.

CAS D'USAGE

Il est impératif de garder une facilité d'accès aux applications et aux données personnelles sensibles sans pour autant altérer la sécurité du Système d'Information, de la chaîne de confiance et sans exposer l'établissement de santé à des fuites de données massives.

- **Savoir gérer le turnover** des équipes et des prestataires externes,
- **Contrôler les identifiants génériques et les comptes partagés :** chaque connexion est imputable à un utilisateur et le contenu de la session est enregistré,
- **Fournir une politique d'authentification souple et contrôlable selon les profils utilisateurs :** changements de mot de passe, utilisation de mécanismes d'authentification adaptés à l'environnement client, gestion des accès distants et des applications dans le cloud,
- **Tracer les actions réalisées, auditabilité :** enregistrement des sessions en vidéo ou texte avec possibilité de les rejouer en cas de litige, accès aux journaux infalsifiables d'audit et de connexions,
- **Mettre en place une politique de surveillance des accès :** alerte en temps réel sur des commandes, du contenu, des accès, avec création d'un reporting automatisé,
- **Assurer une continuité de service :** haute disponibilité, plan de reprise de l'activité avec synchronisation des informations.