



Un clausier de conformité numérique co-construit : une réponse collective aux enjeux de cybersécurité



Béatrice BERARD

*Présidente du Club des RSSI en Santé
Officier de sécurité - DSII
Hospices Civils de Lyon*

Un besoin partagé face à la complexité croissante des exigences

Dans un contexte de montée en puissance des exigences réglementaires en cybersécurité et de multiplication des référentiels (PGSSI-S, NIS2, ISO 27001, HDS, etc.), les établissements, notamment du secteur de la santé, peinent parfois à homogénéiser leurs pratiques contractuelles.

La rédaction de clauses de sécurité adaptées, précises et juridiquement solides, devient un exercice technique et chronophage.

C'est dans ce contexte qu'est née l'idée d'un clausier de conformité numérique ¹ mutualisé, conçu par un collectif d'experts réunissant trois organisations professionnelles : le Club des RSSI en Santé, le Réseau des DPO hospitaliers et l'Association Française des Ingénieurs Biomédicaux. Leur ambition : mettre en commun leurs expériences et besoins pour créer un outil

opérationnel, réutilisable et évolutif, au service de tous.

Une démarche collaborative et structurée

Le projet de clausier a vu le jour grâce à l'initiative d'un groupe de travail composé de RSSI inter-établissements, alimenté par le modèle de clausier utilisé à l'Assistance Publique des Hôpitaux de Marseille (APHM) et appuyé par le soutien de la Centrale d'Achat de l'informatique Hospitalière (CAIH).

Il s'inscrit dans une logique de travail en commun, animée par les principes suivants :

- **Transparence** : toutes les propositions sont discutées en groupe, puis arbitrées collectivement.
- **Pragmatisme** : les clauses sont conçues pour être applicables sur le terrain, adaptées à différents contextes (prestations de services, fourniture de logiciels, maintenance, infogérance, etc.).
- **Interopérabilité** : le clausier s'appuie sur des référentiels reconnus et facilite leur intégration dans les documents contractuels.
- **Accessibilité** : le contenu est rédigé dans un langage clair, structuré par thématique.

Contenu et structure du clausier

Le clausier final se présente comme un document modulaire, organisé en plusieurs sections thématiques :

- **Clauses générales de sécurité** : référentiels applicables, responsabilités des parties.
- **Gestion des identités et des accès** : cycle de vie des identités numériques, droits d'accès, authentification, traçabilité.
- **Protection des données** : conformité RGPD, mesures de pseudonymisation et de chiffrement.

¹ A retrouver [ICI](#)



- **Exigences techniques** : sécurité des systèmes, des flux, des postes de travail, des réseaux.
- **Exigences spécifiques** : télémaintenance, cloud, sous-traitance, dispositifs médicaux, Intelligence artificielle.

Chaque clause est accompagnée de commentaires explicatifs et de recommandations d'usage, permettant à l'utilisateur de mieux en comprendre les enjeux, les modalités d'application et les points de vigilance.

Un outil vivant, mis à jour collectivement

Conscients de l'évolution rapide des menaces et des normes, les membres du collectif ont voulu inscrire le clausier dans une logique d'amélioration continue. Un comité de suivi est chargé d'actualiser le contenu annuellement au fil des évolutions juridiques, technologiques et réglementaires.

Le site web du Club des RSSI en santé² permet à chacun d'accéder au clausier. Chacun peut proposer des modifications, signaler des cas d'usage en écrivant à contact@listes.rssi-sante.fr, afin de mutualiser les bonnes pratiques.

Cette gouvernance ouverte garantit que le clausier reste pertinent, opérationnel et conforme aux exigences du terrain.

Des bénéfices concrets pour les établissements et leurs partenaires

L'utilisation de ce clausier présente de nombreux avantages :

- **Gain de temps** : les équipes juridiques et techniques partent d'une base solide, validée collectivement.
- **Harmonisation** : les exigences de sécurité sont alignées entre les établissements, ce qui facilite les échanges avec les prestataires.
- **Sécurisation juridique** : les clauses sont rédigées dans une logique contractuelle robuste, limitant les zones d'ambiguïté.

- **Dialogue constructif avec les fournisseurs** : les clauses sont expliquées et contextualisées, favorisant une meilleure compréhension et adhésion des partenaires.

Un modèle reproductible dans d'autres domaines

Au-delà du domaine de la cybersécurité, cette expérience de co-construction d'un clausier ouvre la voie à des formes nouvelles de collaboration entre acteurs publics, fondées sur l'entraide, la mutualisation et la transparence.

Le clausier Conformité Numérique n'est pas seulement un outil technique : c'est le reflet d'une culture de la résilience collective, où chaque acteur, quelle que soit sa taille ou sa maturité, peut contribuer à élever le niveau global de sécurité.

Conclusion

Ce clausier Conformité Numérique n'est pas figé. Il vit, s'adapte, se partage. Il incarne une réponse concrète, humaine et pragmatique à un défi technologique complexe. En misant sur la coopération, le collectif a transformé une contrainte en levier de transformation positive.

² A retrouver [ICI](#)