

Groupe de travail mise en œuvre du règlement européen sur la protection des données personnelles (RGPD) dans les laboratoires de Biologie médicale.

La loi de modernisation de notre système de santé du 26 Janvier 2016 et le décret 2016-46 relatif à la biologie médicale ont modifié profondément le régime d'échange et de partage de donnée entre professionnel de santé et le compte rendu de biologie médicale dématérialisé conforme au cadre d'interopérabilité des systèmes d'information de santé (CI-SIS).

Parallèlement à cette incitation à la dématérialisation et à l'échange et au partage de données, le cadre réglementaire sur la protection des données a été redéfinie par le règlement européen sur la protection des données personnelles (RGPD) qui renforce de manière conséquente les sanctions encourues par les entreprises en cas de divulgation de données personnelles (4 % du CA annuel ou 20 millions d'euros).

C'est dans cette environnement très contraint que la SFIL en accord avec la CNIL a décidé d'élaborer un référentiel sectoriel appliqué à la biologie médicale.

Un groupe de travail a été constitué ; composé de biologiste du secteur privé et public, d'éditeurs de logiciels, de représentant du SIDIV de la CNIL et de la SFIL. L'animation est assurée par la société Provadys spécialisée en sécurité informatique et le cabinet Lexing spécialisé en droit du numérique. Le premier travail de ce groupe a été de recenser de manière exhaustives les exigences réglementaires et normatives qui s'appliquent aux professionnels de santé et plus particulièrement aux laboratoires de Biologie médicale. Dans un document de près de deux cents pages ces exigences ont été contextualisées et des recommandations de mises en œuvre ont été proposés en s'appuyant les différentes recommandations de bonnes pratiques proposées par la PGSSI, l'ANSSI et la CNIL. Ce groupe de travail pragmatique, a décliné les exigences spécifiques (réglementaires, ordinales, normatives) au contexte métier de manière opérationnelle pour l'ensemble des typologies de laboratoire.

Dans un deuxième temps nous allons produire un référentiel de conformité d'ici fin 2018 dont l'architecture sera comparable à norme iso 15189, rattaché à ce référentiel nous allons produire une boite à outil facilitant la mise en conformité :

- PIAF (Private Impact Assessment Framework)
- Des documents d'accompagnements :
 - Charte de protection des données personnelles
 - Modèles de registre des violations de données
 - Une convention de preuve
 - L'affichage obligatoire
 - Les clauses obligatoires devant figurées dans un contrat avec un sous-traitant te un cotraitant
 - Lettre de nomination d'un Délégué à la protection des données personnelles (DPD)
 - Modèle de clause devant être introduite dans le contrat de travail du DPD
 - Modèle d'information aux patients
 - Procédure d'information des patients
 - Procédure de gestion des accès
 - Procédure interne de gestion des incidents de sécurité
 - Modèle de registre de traitement

Les premiers documents vont être diffusés dès la fin 2018.