Avis de la Commission nationale pour la protection des données relatif au règlement interne du Registre National du Cancer.

Délibération n° 606/2013 du 23 décembre 2013

Conformément à l'article 2 paragraphe (3) du règlement grand-ducal du 18 avril 2013 déterminant les modalités et conditions de fonctionnement du registre national du cancer, le règlement interne, qui contiendra outre la charte de sécurité, aussi les modalités de contrôle qualité à opérer et les modalités relatives à la publication des résultats est soumis pour approbation au ministre ensemble avec la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale »)

Par courrier du 14 octobre 2013, le Centre de recherche public de la santé (ci-après désigné CRP-Santé), a invité la Commission nationale à se prononcer au sujet des documents concernant le règlement interne du Registre National du Cancer. Le règlement interne, tel que soumis à la Commission nationale, est composé du document du règlement interne (version du 9 octobre 2013), de la charte de sécurité des systèmes d'information (version du 9 octobre 2013), du manuel qualité (version du 25 juillet 2013), de la procédure de diffusion des résultats (version du 9 octobre 2013) et de la brochure d'information des patients.

- Concernant le document de la charte de sécurité, la Commission nationale formule les suggestions suivantes :

1) Au chapitre 3 section « 3.2 Engagements des collaborateurs », il est précisé que « *Lors de son engagement en tant que collaborateur au sein du RNC, il bénéficie de la part du responsable opérationnel du RNC d'une formation, entre autre relative à la sécurité des données, au respect de la confidentialité, au devoir de protection des données à caractère personnel des patients et des sources, et aux procédures inhérentes à ces aspects.* ». La Commission nationale suggère d'étendre cette activité par la mise en place d'une formation continue relative à la sécurité suivant un cycle au minimum annuel. Les risques évoluent et les procédures sont changées pour s'adapter à l'évolution de l'environnement. Le feedback des collaborateurs par rapports aux risques de sécurité et la mise en application de ces procédures peuvent apporter des éléments pertinents quant à la gestion de la sécurité du système d'information. Dans ce contexte, la Commission nationale propose d'organiser une formation mise à jour, au minimum annuellement, relative à la sécurité propre à l'environnement en question.

2) Au chapitre 4 section « II.2. Utilisation professionnelle / privée », il est indiqué que « *L'utilisation résiduelle du système d'information du RNC à titre privé est strictement interdite* ». Il est quasiment inévitable qu'un utilisateur accède à un moment ou à un autre à des sites Internet non professionnels, communique par email avec des correspondants personnels ou effectue une tâche privée avec son PC. De plus, il est de jurisprudence constante que le salarié a droit, dans une certaine mesure, même au temps et au lieu de travail, au respect de sa vie privée, ce qui ne permet pas à l'employeur d'appliquer une restriction totale quant à l'utilisation raisonnable d'un système d'information à titre privé. A ce titre, la Commission nationale recommande de mettre en place des « bornes Internet », séparées du système d'information du RNC, destinées à un usage privé (ex : utilisation de webmails privés, consultation de sites Internet non professionnels) et d'associer à cette activité une charte d'utilisation des bornes Internet.

   De manière générale, la CNPD estime nécessaire d'isoler le système d'information propre au registre national du cancer de toutes autres activités nécessitant l'utilisation d'un système d'information (navigation Internet, email, gestion administrative,...)

3) Le chapitre 4 section « II.4.2 Respect des engagements de la CNPD », précise que « *Le CRP-Santé et ses partenaires s'engagent à respecter les dispositions présentées et validées par la CNPD pendant toute la durée d'exploitation du RNC* ». La Commission nationale suggère de retirer ce texte qui par l'expression « *dispositions présentées et validées par la CNPD* » ne permet pas de déterminer quelles sont les dispositions concernées et peuvent prêter à confusion quant à l'application de la législation sur la protection des données à caractère personnel. En effet, cette dernière est applicable dans son ensemble sous la responsabilité du CRP-Santé (accountability).

4) Le chapitre 4, article III, section « III.1. Règles de sécurité applicables » a trait, entre autres, à la gestion des mots de passes.

   a. Concernant le point « *Le choix d'un mot de passe non trivial* », nous proposons de mettre en place une politique de construction de mots de passe forcée techniquement, afin que les utilisateurs soient contraints d'utiliser des mots de passe avec le niveau de complexité requis.

   b. Il convient de souligner qu'au regard de la sensibilité des données traitées et du caractère national du registre, la sécurité des accès à la base de données du RNC basée uniquement sur la combinaison nom d'utilisateur / mot de passe n'est pas d'un niveau de sécurité suffisant, même si le mot de passe diffère pour l'accès à la base de données du RNC du mot de passe d'accès au terminal de l'utilisateur.

Dans ce contexte la CNPD exige la mise en œuvre d'une authentification forte pour l'accès à la base de données du RNC.

En effet, depuis la survenance de l'incident dit « Medicoleak » au début de l'année 2012, le Cyber Security Board (mis en place par le gouvernement en juillet 2011) a renforcé ses efforts en vue de la mise en œuvre progressive de la politique du gouvernement en matière de cyber sécurité auprès des organismes publics qui gèrent des fichiers contenant des données sensibles. A cet effet, le Cyber Security Board s'est prononcé « *pour une généralisation obligatoire du système de l'authentification forte pour les applications sensibles notamment via l'application LUXTRUST* ». Ainsi, au fur et mesure de leur identification, les bases de données « sensibles », gérées par les administrations et établissements publics, devront obligatoirement être équipées d'une authentification forte Luxtrust.

De l'avis de la CNPD ceci devra évidemment aussi être le cas pour une base de données aussi sensible que le Registre National du Cancer dont la gestion est assurée par le Centre de Recherche Public de la Santé.

Dans cette même section, la charte de sécurité énumère un certain nombre de règles élémentaires à appliquer par le collaborateur, « *De la part du collaborateur* », pour lesquelles la Commission nationale suggère d'appliquer les mesures suivantes:

c. « *ne pas connecter aux réseaux locaux des équipements non autorisés par le CRP-Santé ou son établissement* » : nous conseillons la mise œuvre de blocages techniques pour appliquer cette mesure et ne pas en laisser le contrôle uniquement aux utilisateurs.

d. « *ne pas déposer les données relatives aux RNC…* » : la CNPD suggère de ne pas laisser aux utilisateurs la possibilité d'évaluer eux-mêmes les conséquences de tels actes. A cet effet, nous conseillons de définir une procédure précise, comprenant les instructions d'acceptation des cas où les données professionnelles peuvent être déposées en dehors du système d'information du Registre National du Cancer. Cette procédure pourra se référer au document de « Procédure de diffusion des résultats », mais elle devrait également prendre en compte les activités quotidiennes des collaborateurs pour lesquelles une exportation des données entre ligne de compte (exemples : stockage intermédiaire de données, données nécessaires pour une activité exceptionnelle ou liée à l'administration quotidienne.

e. « *assurer la protection des informations sensibles du RNC et ne pas les transporter sans protection …* » : Comme pour le point « c » ci-avant, la Commission nationale conseille l'implémentation d'un outil qui permet le contrôle des supports mobiles (contrôle de l'utilisation et obligation du chiffrement de ces supports). Cet outil devra également être en mesure de forcer techniquement l'application de cette règle.

f. « *ne pas quitter son poste de travail… sans se déconnecter ou verrouiller sa session par un mot de passe*» : la Commission nationale recommande d'ajouter la mise en œuvre d'un blocage automatique de la station après quelques minutes d'inactivité.

5) Au chapitre 4, article III, section « III.2 Devoirs de signalement et d'information », la charte de sécurité indique que le « *collaborateur doit avertir le CRP-Santé dans les meilleurs délais en cas de découverte d'une anomalie affectant le système d'information* ». A cet effet, la CNPD propose d'indiquer aux collaborateurs un point de contact unique (SPOC – Single Point Of Contact) auquel les collaborateurs peuvent s'adresser en cas de suspicions d'incident ou d'incident avéré. Dans la continuité de ce processus, nous conseillons fortement de créer et d'implémenter une procédure de gestion des incidents dans laquelle sont, entre autres, définis les rôles et responsabilités de chacun, les flux de communication et les pouvoirs décisionnels en cas de survenance d'un incident.

6) Dans le chapitre 4, article IX « Transmission des données électroniques vers le RNC », la Commission nationale voudrait relever une erreur de syntaxe dans l'expression « *modèle de cryption par clé asymétrique* » et suggère de remplacer cette expression par « modèle de chiffrement asymétrique »

7) Dans le chapitre 4, article XII « Réalisation d'un audit de sécurité », concernant le point « *un audit externe commandité à une société indépendante qualifiée en sécurité informatique* », il conviendrait de remplacer le terme « sécurité informatique » par « sécurité de l'information ». L'objectif étant d'éviter que ces audits externes ne soient purement techniques, mais prennent également en compte les aspects organisationnels de gestion de la sécurité de l'information.

8) La Commission nationale souhaite également relever les points suivants pouvant être ajoutés à la charte de sécurité :

   a. Nous conseillons d'intégrer une section relative à l'utilisation du téléphone et d'indiquer aux collaborateurs les règles de divulgations et de collectes d'information par téléphone.

   b. La même remarque vaut pour les communications liées à l'utilisation des courriels.

c. Finalement, nous suggérons également d'insérer une section sur la mise en œuvre de mesures relatives à la continuité de service et la récupération de production (BCP / DRP).

- Concernant le document de « Convention de transfert de données », la Commission nationale émet les remarques suivantes :

En ce qui concerne l'article 11 section 11.2 « Incidents », nous renvoyons aux recommandations du point 5) de la section précédente en mettant en œuvre une procédure commune de gestion des incidents.

- Concernant le formulaire de refus du patient :

La CNPD estime important et nécessaire de rajouter au formulaire de refus du patient une phrase qui informe le patient que son opposition au traitement de ses données n'entraîne aucun préjudice pour lui et ne porte pas atteinte à son droit à recevoir des soins de santé appropriés, conformément à l'article 4 paragraphe (1) 2ème alinéa du règlement grand-ducal du 18 avril 2013 déterminant les modalités et conditions de fonctionnement du registre national du cancer.

Ainsi décidé à Esch-sur-Alzette en date du 23 décembre 2013.

La Commission nationale pour la protection des données

Gérard Lommel Président	Pierre Weimerskirch Membre effectif	Thierry Lallemang Membre effectif