Délibération n° 2023-111 du 20 septembre 2023

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Portail patient du CHPG* »

présenté par le Centre Hospitalier Princesse Grace

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 127 du 15 janvier 1930 constituant l'hôpital en établissement public autonome ;

Vu la Loi n° 918 du 27 décembre 1971 sur les établissements publics ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 5.095 du 14 février 1973 sur l'organisation et le fonctionnement du Centre Hospitalier Princesse Grace, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu la délibération n° 2011-82 du 21 octobre 2011 portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Centre Hospitalier Princesse Grace, le 24 mai 2023, portant sur la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Portail patient du CHPG* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 21 juillet 2023, conformément à l'article 19 l'Ordonnance Souveraine n° 2.230 du 19 juin 2009, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 20 septembre 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Aux termes de la Loi n° 127 du 15 janvier 1930, le Centre Hospitalier Princesse Grace (CHPG) est un établissement public autonome.

Afin de permettre aux patients d'accéder plus facilement à un certain nombre de services et de documents médicaux, le CHPG souhaite mettre en place un espace sécurisé sur son site Internet.

Le traitement d'informations nominatives objet de la présente délibération est donc soumis à l'avis de la Commission conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement indique que le traitement a pour finalité « *Portail patient du CHPG* ».

Les personnes concernées sont les patients, les secrétaires médicales et les médecins.

Enfin, les fonctionnalités sont les suivantes :

- création de l'espace patient (le CHPG créé cet espace qui est ensuite activé par le patient) ;
- gestion des rendez-vous (prise de rendez-vous, visualisation et annulation des rendez-vous déjà pris, alerte SMS et/email pour le rappel des rendez-vous) ;
- pré-remplissage des informations concernant la préadmission ;
- accès aux documents médicaux (comptes-rendus de consultation, résultats laboratoires, lettres de liaison) ;
- questionnaires médicaux et de satisfaction liés au portail patient ;
- paiement en ligne des factures.

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

Ce traitement est justifié par un motif d'intérêt public afin de permettre au CHPG d'assurer « *sa mission de service public dans l'intérêt de ses patients et pour répondre aux besoins de la santé publique* ».

Le responsable de traitement précise en outre qu'il « *permet de faciliter la prise en charge du patient par la création automatique de son espace (accès centralisé à ses informations)* ».

La Commission considère ainsi que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Le responsable de traitement indique que les informations nominatives traitées par le portail de manière automatisée sont :

- identité :
  - patient : sexe, nom usuel, nom de naissance, prénom, date de naissance, justificatif d'identité, téléphone, email, numéro de sécurité sociale ;
  - médecin, personne de confiance, personne à prévenir : nom, prénom ;
- adresses et coordonnées : adresse complète, téléphone(s) ;
- formation, diplômes, vie professionnelle : spécialité, examens, motif de consultation (bilan de syncope publique, cardiologie générale publique, …), lettre du médecin, texte champ libre (« *Laissez-nous un message* ») ;
- données d'identification électronique : logs de connexion ;
- informations du rendez-vous : date et heure du rendez-vous, affichage d'autres horaires, affichage plan d'accès CHPG ;
- couverture sociale : caisse d'assuré social, copie d'attestation de droits en cours de validité (caisse sociale, mutuelle), date de l'accident de travail/maladie professionnelle, numéro de sécurité sociale ;
- facturation : numéro de facturation, numéro du titre, montant, numéro de carte bancaire, état du paiement par carte bancaire ;
- questionnaires de satisfaction (facultatif) : date hospitalisation, intervention, consultation pré anesthésique (oui/non), satisfaction globale (pas satisfait : 0 à très satisfait : 10), « *Vous a t'on remis le passeport ambulatoire lors de votre consultation chez l'opérateur (oui/non) ?* », « *Avez-vous eu un contact téléphonique la veille de votre venue ?* » (oui/non), degré de satisfaction concernant les informations et explications données par l'opérateur (smiley) ;
- questionnaire pré opératoire : « *Avez-vous réalisé votre préadmission ?* » (oui/non), dans le cadre d'une anesthésie générale, « *la consultation pré-anesthésie a t-elle été réalisée* ? » (oui/non), « *Avez-vous réalisé votre test PCR ?* » (oui/non), état de santé, (…) ;
- identifiants de connexion au portail : adresse email et mot de passe complexe ;
- données de santé : comptes rendus de consultation, réslutats laboratoires, lettres de liaison, questionnaires médicaux.

Les informations relatives à l'identité ont pour origine le patient et le justificatif d'identité.

Les informations relatives aux adresses et coordonnées, les réponses aux questionnaires et les identifiants de connexion au portail ont pour origine le patient.

Les informations relatives à la formation, aux diplômes et à la vie profesisonnelle ont pour origine les médecins.

Les logs de connexion ont pour origine le système.

Les informations relatives à la couverture sociale ont pour origine le patient et la carte d'assuré social.

Les informations relatives à la facturation ont pour origine le traitement ayant pour finalité « *Gérer les dosiers administratifs des patients* », le patient et la banque (pour l'état de paiement uniquement).

Les données de santé ont pour origine le patient, les médecins et les laboratoires.

Enfin, la Commisison considère que les informations liées au rendez-vous ont pour origine le portail.

La Commission considère ainsi que les informations collectées au sein dudit traitement sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

- ***Sur l'information préalable des personnes concernées***

L'information préalable des personnes concernées est réalisée par le biais de la *« Politique de protection des données à caractère personnel du CHPG »* du site Internet du CHPG et de la rubrique *« vos droits et devoirs »* du livret d'accueil du patient.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle que l'information des personnes concernées doit impérativement être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès des personnes concernées par le traitement s'exerce par courrier électronique auprès du Délégué à la protection des données.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, la Commission constate ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165 du 23 décembre 1993.

V. Sur les personnes ayant accès au traitement

Les personnes pouvant avoir accès aux informations sont :

- les administrateurs DSIO : tous les droits dans le cadre de leurs missions de maintenance et de sécurité ;

- le prestataire : tous droits dans le cadre de la maintenance (sous le contrôle de la DSIO).

Il appert par ailleurs à l'analyse du dossier que les patients ont également accès à leur espace ainsi qu'à certaines informations médicales les concernant.

Au vu des missions et attributions de chacune des personnes ayant accès au traitement, la Commission considère que les accès sont justifiés, et donc conformes aux dispositions de la Loi n° 1.165 du 23 décembre 1993.

En ce qui concerne le prestataire, elle rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

VI. Sur les rapprochements et interconnexions

Le responsable de traitement indique que le présent traitement fait l'objet de cinq rapprochements avec les traitements ayant respectivement pour finalité « *Gérer les dossiers administratifs des patients* », « *Dossier médical du patient informatisé », « Gestion du site Internet du CHPG », « Gestion de la messagerie professionnelle du CHPG »* et *« Gestion des enquêtes de satisfaction du CHPG ».*

Le présent traitement est également interconnecté avec le traitement ayant pour finalité « *Gestion des rendez-vous patients et logistique médicale* ».

La Commission constate que ces traitements ont été légalement mis en œuvre.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observations.

La Commission rappelle toutefois que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Elle rappelle enfin que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur les durées de conservation

Le responsable de traitement indique que toutes les données rattachées au dossier et aux séjours des patients sont conservées 20 ans à partir de la dernière visite à l'hôpital.

Il indique par ailleurs que les logs de connexions sont conservés 1 an et les réponses aux questionnaires de satisfaction 2 ans.

Les informations relatives à la facturation sont conservées 13 mois à compter de la date de débit à l'exception des informations concernant la carte bancaire qui sont conservées le temps de traitement du paiement.

Enfin, les identifiants de connexion au portail sont conservés jusqu'à la suppression du portail patient.

La Commission considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- l'information préalable des personnes concernées doit impérativement être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre, par le Centre Hospitalier Princesse Grace, du traitement automatisé d'informations nominatives ayant pour finalité *« Portail patient du CHPG ».***

Le Président

Guy MAGNAN