DÉCLARATION DE CONFORMITÉ RELATIVE À LA SÉCURITÉ DU SYSTÈME D'INFORMATION FAISANT L'OBJET D'UNE DEMANDE D'AUTORISATION OU D'ADHÉSION

A compléter par l'institution et retourner à:

Comité de sécurité de l'Information Chambre Sécurité Sociale et Santé
A l'attention de Joke Vanderpoorten
Quai de Willebroeck - 1000 Bruxelles
Tel. : 02/ 741.84.27
E-mail : ivc@mail.fgov.be

Cette déclaration de conformité concerne :

☐ Une nouvelle demande d'autorisation

☐ Une autorisation déjà accordée par la délibération

☐ Une demande d'adhésion à l'autorisation générale accordée par

☐ Les délibérations pour **les maisons de repos ou de soins agréées** :
N° 11/084 du 08/11/2011 du Comité sectoriel de la Sécurité Sociale et de la Santé
N° 41/2011 du 20/07/2011 du Comité sectoriel du Registre national

☐ Délibérations pour **les maisons de soins psychiatriques et les initiatives d'habitation protégée b**
Nr. 11/083 du 08/11/2011 du Comité sectoriel de la Sécurité Sociale et de la Santé
Nr. 40/2011 du 20/07/2011 du Comité sectoriel du Registre national

☐ Délibérations pour **les laboratoires agréés de biologie clinique** :
Nr. 10/078 du 09/11/2010 du Comité sectoriel de la Sécurité Sociale et de la Santé
Nr. 35/2010 du 06/10/2010 du Comité sectoriel du Registre national

☐ Délibérations pour **les hôpitaux** :
Nr. 09/039 du 07/07/2009 du Comité sectoriel de la Sécurité Sociale et de la Santé
Nr. 21/2009 du 25/03/2009 du Comité sectoriel du Registre national
Nr. 60/2009 du 07/10/2009 extension de n°. 21/2009 du 25/03/2009 du Comité sectoriel du Registre national

Autre :

……

……

Organisme demandeur responsable du traitement	
Nom	
Abréviation officielle	
Adresse officielle	
Numéro d'entreprise (BCE)	
Numéro de l'unité d'établissement (BCE)	
Numéro INAMI	
Numéro EHP[1]	

Responsable de la gestion journalière du traitement	
Coordonnées	
Titre	
Nom	
Prénom	
Adresse de contact	
Téléphone	
e-mail	
Langue	

Je soussigné, responsable de la gestion journalière du traitement de données à caractère personnel faisant directement l'objet de la demande d'autorisation ou d'adhésion à une autorisation générale, ci-après : 'le traitement en question',

certifie que, pour le traitement en question, et conformément aux obligations prévues par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 30 juillet 2018 et les autres lois en vigueur, et comme le recommandent les Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel éditées par la Comité de Sécurité de l'Information,

les mesures techniques et organisationnelles appropriées ont été mises en place de façon à être opérationnelles, au plus tard pour la date de mise en exécution de ce traitement, de manière à assurer un niveau de protection adéquat des données à caractère personnel traitées tout en tenant compte,

- de la nature des données à caractère personnel traitées et de leur traitement ainsi que des exigences en matière de confidentialité, intégrité et disponibilité ;
- des exigences légales ou réglementaires qui seraient d'application ;
- de la taille de l'organisme (incluant le nombre et le profil des personnes susceptibles d'accéder aux données) ;
- de l'importance et de la complexité des systèmes d'information, systèmes informatiques et applications concernés ;
- de l'ouverture de l'organisme vers l'extérieur ainsi que des accès depuis l'extérieur ;
- des risques encourus tant pour l'organisme lui-même que pour les personnes dont les données à caractère personnel sont traitées ;
- de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures ;

[1] Uniquement pour les établissements de soins agréés par un numéro EHP.

certifie que, au plus tard pour la date de mise en exécution de ce traitement, les aspects suivants de la sécurité auront été finalisés (cocher la case correspondante) :

1. **Le délégué à la protection des données (DPO) nommé dans cette institution est chargé de la mise en œuvre de la politique de sécurité pendant le traitement des données** **OUI ☐ NON ☐**

Coordonnées du délégué à la protection des données (DPO)	
Nom	
Prénom	
e-mail	

Le DPO a été notifié avec succès à l'autorité de protection des données (APD) OUI ☐ NON ☐

Le DPO a été notifié avec succès à Plate-forme eHealth OUI ☐ NON ☐

2. **L'évaluation des riques** **OUI ☐ NON ☐**

   Une évaluation des risques encourus par les données à caractère personnel traitées a été réalisée et les besoins de sécurité ont été définis en conséquence et appliqués.

3. **La politique de sécurité de l'information** **OUI ☐ NON ☐**

   Un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser les données à caractère personnel traitées a été élaboré.

4. **L'identification du personnel** **OUI ☐ NON ☐**

   Tous les supports, quels qu'ils soient et contenant les données à caractère personnel traitées, ont été identifiés.

5. **L'information du personnel** **OUI ☐ NON ☐**

   Le personnel interne et externe impliqué dans ce traitement a été informé de ses devoirs de confidentialité et de sécurité vis-à-vis des données à caractère personnel traitées découlant aussi bien des différentes exigences légales que de la politique de sécurité

6. **La sécurisation physique des accès** **OUI ☐ NON ☐**

   Des mesures de sécurité adéquates ont été mises en place afin de prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel traitées.

7. **La sécurité physique et environnementale** **OUI ☐ NON ☐**

   Les mesures de sécurité nécessaires ont été mises en place afin de prévenir les dommages physiques pouvant compromettre les données à caractère personnel.

8. **La sécurisation des réseaux** **OUI ☐ NON ☐**

   Les différents réseaux auxquels sont reliés les équipements traitant les données à caractère personnel sont protégés.

9. **La liste des personnes habilitées** **OUI ☐ NON ☐**

   Une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel dans le cadre de ce traitement, reprenant leur niveau d'accès respectif (création, consultation, modification, destruction), a été établie.

10. **La sécurisation logique des accès** **OUI ☐ NON ☐**

    Un mécanisme d'autorisation d'accès conçu de façon à ce que les données à caractère personnel traitées et les traitements les concernant ne soient accessibles qu'aux personnes et applications explicitement autorisées a été mis en place.

11. **La journalisation des accès** **OUI ☐ NON ☐**

    Le système d'information a été conçu de façon à permettre une journalisation, un traçage et une analyse permanents des accès des personnes et entités logiques aux données à caractère personnel traitées.

    Le cas échéant, une attention suffisante aura été portée aux aspects suivants de la sécurité.

12. **La surveillance, la révision et la maintenance** **OUI ☐ NON ☐**

    Un contrôle de la validité et de l'efficacité dans le temps des mesures techniques ou organisationnelles mises en place a été prévu.

13. **La gestion d'urgence des incidents de sécurité de l'information** **OUI ☐ NON ☐**

Des procédures de gestion d'urgence des incidents de sécurité impliquant les données à caractère personnel traitées ont été mises en place.

14. La documentation **OUI ☐ NON ☐**

Une documentation suffisante concernant l'organisation de la sécurité de l'information dans le cadre du traitement en question a été constituée et sera tenue à jour.

Je certifie sur l'honneur que les renseignements fournis sont conformes à la réalité [2].

Nom :

Date :

Signature :

[2] Toute déclaration non conforme à la réalité peut être considérée comme un faux en écriture engageant la responsabilité pénale du responsable du traitement. Les documents sont tenus à la disposition du Comité de Sécurité de l'Information qui peut en demander copie ou procéder à un examen sur place pour vérifier l'état de la sécurité de l'information.