



Security Policy

CONFIDENTIALITE, SECURITE DES DONNEES AIM ET LE SECRET PROFESSIONNEL

Directives pour les personnes qui participent à des projets AIM

Cadre

Introduction

L'Agence Intermutualiste (AIM) reçoit régulièrement des informations confidentielles et souvent sensibles concernant la sécurité sociale. Ces informations sont mises à notre disposition par le biais de divers canaux, principalement les OA. Nous en avons besoin pour pouvoir remplir les missions qui nous sont confiées.

Il convient d'être très attentifs lorsque nous sommes confrontés à ces données AIM¹, non seulement pour nous conformer aux obligations légales en la matière, mais également pour des motifs éthiques. Chaque collaborateur à un projet AIM est responsable dans ses activités quotidiennes du respect de nos obligations et de notre politique en matière de protection des données.

Nous sommes convaincus que vous mettez actuellement déjà tout en œuvre pour honorer cette responsabilité. Ce texte de base contient un ensemble de directives pour vous y accompagner. Nous souhaitons par ce biais vous sensibiliser (préventivement) et limiter de la sorte des interventions en cas de non respect de ces directives.

Ce texte vaut pour tous les utilisateurs des informations transmises à l' AIM qu'elles soient détaillées ou agrégées. Il a été établi par le groupe de travail sur la protection des données, adapté par le comité de pilotage et de coordination et ensuite validé par le conseil d'administration de l' AIM.

La direction de chaque entité est responsable de l'application des directives en ce qui concerne les aspects organisationnels quotidiens. Elle s'engage à prévoir les moyens nécessaires pour garantir une application correcte, entre autre en assurant une formation pour chaque collaborateur ayant accès aux données.

Nous comptons sur vous pour l'application stricte de ces directives.

Marc Justaert
Président du conseil d'administration

Patrick Verertbruggen
Secrétaire

¹ Quoique, au niveau des bases de données AIM, l'identificateur du patient est toujours protégé par un double encodage par deux instances indépendantes, il s'agit néanmoins souvent de données qui ont un caractère personnel. De plus, à l'occasion de certains projets les données peuvent également être considérées comme des données, concernant les prestataires ou prescripteurs, à caractère personnel.



Security Policy

Suite à la page suivante



Security Policy

Cadre, Suite

Contenu

Cette note traite les sujets suivants.

Sujet	Voir page
Localisation	1
Sécurité et protection des données AIM et le secret professionnel	3
Premier principe : que pouvez-vous consulter ?	4
Deuxième principe : l'utilisation de données AIM	5
Troisième principe : combien de temps pouvez-vous conserver les données AIM ?	6
Quatrième principe : vous êtes tenu par le secret professionnel	7
Traitement de données AIM	8
Données médicales et le rôle du médecin responsable AIM	9

Quid en cas de non-respect ?

Le non respect des directives prévues par le présent texte de base sera considéré comme une faute professionnelle et peut être sanctionné sur la base des procédures de licenciement en vigueur dans chaque institution amenée à traiter des données dans le cadre de l' AIM.

Puisque les directives reprises dans ce texte de base s'appuient en grande partie sur des textes légaux (cfr. page suivante), certaines violations peuvent impliquer des poursuites pénales, tant pour l'employeur que pour l'employé.

Spécifiquement pour le secret professionnel: celui-ci vaut même après la rupture ou la fin du contrat de travail.

Obligation d'information

Chaque collaborateur se doit de communiquer immédiatement au conseiller en sécurité de projet tout risque ou incident qu'il constate par rapport à la protection des données. La communication doit également être adressée au chef de projet si la constatation est réalisée dans le cadre d'un projet IMA spécifique. Toutes les irrégularités doivent être systématiquement signalées au Président de l'AIM. Si ces irrégularités concernent des données médicales, elles doivent en outre être signalées au médecin responsable AIM¹.

¹ Praticien des soins de santé sous la surveillance et la responsabilité duquel le traitement et l'analyse de données à caractère personnel relatives à la santé sont effectués



Security Policy

Sécurité et protection de données AIM et le secret professionnel

Base légale

Les deux lois suivantes principalement sont d'application à la protection des données personnelles :

- Loi relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (Loi du 15-01-1990).
- Loi relative à la protection de la vie privée à l'égard des traitements de données personnelles (Loi du 8-12-1992).

Par ailleurs, des dispositions concernant la sécurité et la communication des données et le secret professionnel ont également été insérées dans la Loi relative aux contrats de travail, dans les CCT, dans le règlement de travail et dans le code pénal.

Introduction

En vertu de la législation, les institutions collaborant à AIM doivent prendre toutes les mesures utiles afin de garantir le caractère confidentiel des données AIM et peuvent utiliser ces données AIM uniquement afin de remplir leur mission dans le cadre des projets AIM.

En cas de doute concernant l'application correcte de ces mesures, un collaborateur doit consulter son supérieur direct.

4 principes

Ceci signifie que les collaborateurs qui travaillent avec des données AIM doivent respecter quatre grands principes.

Contenu

Les sujets suivants sont développés ci-après :

Sujet	Voir page
Premier principe : que pouvez-vous consulter ?	4
Deuxième principe : l'utilisation de données AIM	5
Troisième principe : combien de temps sont conservées les données AIM ?	6
Quatrième principe : Secret professionnel	7
Traitement de données AIM	8
Données médicales et le rôle du médecin responsable AIM	9



Security Policy

Premier principe : que pouvez-vous consulter ?

Qu'est-ce qui est permis ? Prenez uniquement connaissance des données AIM **dont vous avez besoin** pour remplir votre mission dans le cadre de l' AIM.

En principe, pour chaque projet seront définies : (1) les personnes à qui un accès aux données est octroyé, et (2) pour chaque personne les données spécifiques auxquelles elle a accès pendant une durée déterminée.

Qu'est-ce qui est interdit ? Vous n'avez pas le droit de consulter ou d'essayer de retrouver les données personnelles des personnes suivants:

- un membre de la famille,
 - un collègue,
 - un ami ou une personne que vous connaissez,
 - un prestataire (sauf dans le cadre de la production de feedbacks individuels)
 - une personne connue (par exemple un mandataire politique, une vedette, ...)
 - même les recherches ciblées par curiosité, sont également interdites.
-



Security Policy

Deuxième principe : l'utilisation et le transfert de données AIM

Qu'est-ce qui est permis ? Utilisez les données AIM dont vous avez connaissance uniquement pour remplir votre mission, dans le cadre du projet AIM auquel vous participez.

Qu'est-ce qui est interdit ? Il est **interdit** :

- de transmettre à des tiers, sans autorisation formelle préalable du conseil d'administration, des données AIM sous quelque forme que ce soit, qu'elles soient détaillées ou agrégées ;
- d'utiliser des données AIM à des fins privées (p.ex. dans le cadre d'un litige personnel) ;
- de copier des données AIM sur d'autres supports fixes ou amovibles, ou sur des médias portables, sauf si ceci est explicitement requis et prévu dans le protocole du projet auquel vous participez ;
- de laisser l'accès aux données AIM à des tiers par l'utilisation de votre accès personnel, que ce soit de manière volontaire ou fortuite ;
- d'emporter à domicile des listings informatiques ou autres documents contenant des données AIM pour les utiliser comme papier brouillon ou à dessin.

Transfert de données Le transfert de données entre les différents partenaires AIM est interdit sans autorisation formelle.

La copie des données sous quelque support que ce soit (CD, DVD, clé USB...) est interdite, sauf si ceci est explicitement requis et prévu dans le protocole du projet auquel vous participez.

La consolidation de données AIM et/ou autres est interdite si cette consolidation n'est pas nécessaire dans le cadre du projet auquel vous participez.

Exemples d'utilisation interdite Exemple : Il est interdit de télécharger des bases de données AIM sur votre propre PC fixe ou, à plus forte raison, sur un PC portable pour les traiter localement.

Exemple : Il est interdit de transmettre des résultats intermédiaires d'analyses en cours à d'autres personnes que celles qui sont formellement habilitées à traiter ces informations dans le cadre de leur rôle dans le projet en question.



Security Policy

Troisième principe : combien de temps pouvez-vous conserver les données AIM ?

Qu'est-ce qui est permis ? Vous ne pouvez conserver les données AIM **qu'aussi longtemps que vous en avez besoin pour accomplir vos tâches dans le cadre du projet auquel vous participez.**

Le chef de projet est responsable de faire détruire le plus vite possible les données lors de la clôture du projet, ou dès que celles-ci ne sont plus utiles dans le cadre du projet en question ou d'un projet futur qui est déjà formellement décrit et planifié.

Qu'est-ce qui est interdit ?

- Vous ne pouvez laisser traîner sur votre bureau des listings ou résultats intermédiaires dès que vous n'en avez plus besoin.
- Vous ne pouvez pas conserver des copies de données AIM sur d'autres supports ou médias.

Exemple Il est interdit de conserver une copie du DVD qui sert à transmettre les fichiers d'un feedback CNPQ vers l'imprimeur.



Security Policy

Quatrième principe : vous êtes tenu par le secret professionnel

Secret professionnel

En tant que collaborateur à un projet AIM, vous êtes lié par le secret professionnel.

Ce secret professionnel **vaut à l'égard de** :

- vos collègues (à moins que vous ne deviez échanger ces données AIM avec des collègues en raison de vos affectations réciproques à un même projet AIM) ;
- vos directions ;
- votre propre entourage ou famille ;
- la presse ;
- politiciens ;
- prestataires ou institutions de soins ;
- tiers (amis, connaissances, voisins, relations d'affaires, ...).

Les prestataires, les assurés sociaux et les institutions comptent sur votre discrétion et le respect de leur vie privée !

Caractère confidentiel des informations

Toutes les données AIM dont vous prenez connaissance

- directement ou
- indirectement

dans le cadre de votre tâche dans un projet AIM sont **confidentielles**.

Ceci concerne aussi bien les données brutes que des analyses, résultats et interprétation de ces résultats.

Ces informations ne peuvent en aucun cas être communiquées par un quelconque moyen, que ce soit sous forme de liste, sous forme électronique, par téléphone ou par mail à des tiers au projet auquel vous participez, sans que ceci ait été explicitement prévu dans le protocole du projet.

Exemples

Exemples de données qui ne peuvent pas être communiquées à d'autres personnes ou instances que celles qui ont été formellement prévues dans le protocole du projet en question :

- Le profil d'utilisation de soins ou de prescription d'un prestataire individuel ou d'une institution de soins.
 - Des résultats agrégés montrant des variations entre types de prestataires ou de patients, entre régions ou entre types d'institutions.
-



Security Policy

Traitement de données AIM

Données AIM informatisées

Lors du traitement de données AIM informatisées, trois principes doivent être pris en considération :

- Votre mot de passe est personnel et vous ne pouvez le communiquer à personne. Ne l'inscrivez pas, par exemple, sur le moniteur de votre ordinateur.
 - Si vous connaissez le mot de passe d'un collègue, vous ne pouvez pas l'utiliser. Vous devez en outre le lui signaler, et celui-ci doit le modifier obligatoirement.
 - Modifiez régulièrement votre mot de passe et ne choisissez pas un code évident.
-

Données AIM papier

- Les données AIM ne peuvent rester consultables que pendant le laps de temps nécessaire pour la réalisation du projet.
 - Les données résultat d'un projet ne seront pas conservées au delà du délai fixé dans les objectifs du projet.
 - Aucune donnée AIM ne sera emportée en dehors du lieu de travail. Si, malgré tout, ceci est nécessaire, ces données AIM seront transportées dans une serviette fermée, ne seront jamais abandonnées dans la voiture et seront conservées sous clé.
 - Les supports avec les données AIM ne peuvent être laissés sans surveillance et doivent être mis en sécurité à un endroit protégé.
 - Les mots de passe doivent être conservés sous pli fermé à un endroit protégé.
-

Rôle du chef de projet

Le chef de projet a un rôle important concernant la protection des données AIM et le secret professionnel; ce rôle peut être décrit comme suit :

- Il se charge de l'application des directives.
- Il veille à ce que chaque collaborateur au projet ne puisse accéder qu'aux données AIM informatisées qui sont nécessaires à l'exercice de sa fonction.
- Il conseille les collaborateurs au projet concernant des cas concrets.
- Il donne aux collaborateurs au projet l'autorisation de consulter ou de traiter des données AIM papier qui sont nécessaires à l'exercice de leur fonction. Il révoque cette autorisation dès qu'elle n'est plus nécessaire.
- Il veille à la définition des délais de conservation des données AIM
- Il veille à la destruction des données AIM à la clôture du projet

En cas de modification de fonction ou du contenu des tâches, il veillera à adapter rapidement et correctement les compétences d'accès.



Security Policy

Données médicales et le rôle du médecin responsable AIM

Médecin responsable AIM

Le législateur prévoit une série de mesures spécifiques (plus strictes) pour la protection des données personnelles qui concernent la santé, lesdites données médicales. L' AIM a désigné un praticien des soins de santé sous la surveillance et la responsabilité duquel le traitement et l'analyse de données à caractère personnel relatives à la santé sont effectués. Ce praticien sera ci-après dénommé "médecin responsable AIM"

Quoi?

Sont considérées comme données médicales, toutes données à caractère personnel qui concernent la santé, telles que définies dans l'article 37 de la loi sur la Banque carrefour de la sécurité sociale. Ceci inclut des données dont on peut déduire des informations concernant l'état de santé physique ou mentale passé, présent ou futur.

La protection de ces données est sous la responsabilité du médecin responsable AIM.

Remarque

Pour certaines données AIM, il ne fait absolument aucun doute qu'il s'agit de données médicales (une prestation chirurgicale, une prescription d'un médicament, ...).

D'autres données personnelles AIM (par exemple un profil de prescription d'un médecin) ne doivent pas être considérées comme données médicales.

Rôle du médecin responsable

Selon la loi, les données médicales **ne peuvent être traitées que sous la surveillance et la responsabilité d'un médecin.**

Le médecin responsable AIM est responsable pour le traitement des données médicales. Il est également compétent pour déterminer quelles données AIM doivent être considérées comme données personnelles médicales conformément à la loi.

Dans les différentes organisations participant à AIM, *un médecin responsable* est le garant de l'application de la réglementation et des directives internes. Il signale ses constatations et/ou remarques éventuelles au médecin directeur et au médecin responsable AIM.

Suite à la page suivante



Security Policy

Données médicales et le rôle du médecin responsable AIM, *Suite*

Accès limité

Seul un nombre **limité** de collaborateurs disposent d'une autorisation pour traiter des données médicales.

Les noms de ces personnes, de même que la portée de leur autorisation, sont consignés dans un **registre à l' AIM**.

Tous les autres collaborateurs au projet qui ne nécessitent pas directement ce type d'information n'y ont **pas** accès.
