Questionnaire préalable d’Évaluation des Risques   
pour la sécurité du Système d’Information

**Référentiel Général de sécurité (Décret n°2010-112 Art. 3)**

*☞ Toutes les rubriques doivent être renseignées ☜*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Renseignements sur le demandeur** | | | | **Téléphone** | |
| R1 | **Responsable du traitement** | | Pierre ROUSSEAU, Directeur général de la CPAM 44 |  | |
| R2 | **Nom du projet** | | Gestion des Incidents avec le Public |
| R3 | **Directeur de projet MOA[[1]](#footnote-1)** | | Fabrice Martin, Directeur de la DGSR- Josiane Bouyer- Responsable Accueil, Thomas Hervouet, Manager unité activité service | 02 51 88 84 23 | |
| R4 | **Directeur de projet MOE** | | Frédéric Bougeant, Directeur de la DRHM – François Thorel, responsable du pôle informatique | 02 51 88 85 74 | |
| Date | | 09/11/16 (révision) Enr.24/11/16 - Impr.09/02/12 | | |

# Profil du projet

| *#* | *Thème* | *Réponse de la maîtrise d’ouvrage* | | |
| --- | --- | --- | --- | --- |
| R5 | Domaine du projet ou du service analysé | Interne AM  Relation avec l’extérieur  Pilote, expérimentation  Projet organisationnel  Autre : | | |
| R6 | Échanges envisagés | Au sein de l’organisme  Entre organismes AM  Avec entité(s) hors AM – Autre ou précisions : | | |
| R7 | Sensibilité maximum de l’information traitée | Données nominatives  Médical  Social Autre : | | Finance/comptabilité  Ressources humaines |
| R8 | Utilisateurs | Agents  Assurés/bénéficiaires  Professionnels de la santé  Autres : Agents Pôles accueil physique et téléphonique | | |
| R9 | Aire géographique | Un  Plusieurs organisme(s)  Outre-mer  Précisez : CPAM 44 | | |
| R10 | Partenaires extérieurs | Autres Régimes  autres  Précisez : Pas de partenaires extérieurs | Transfert de données Branche envisagé  Accès aux données Branche envisagé  Précisez : | |
| R11 | Support envisagé | Support Branche  Organisme        Société extérieure  Autre : | | |
| R12 | Importance stratégique pour la Direction générale | Prioritaire  Normale  Date souhaitée de mise en oeuvre : 2012 | | |
| R13 | Nombre d’utilisateurs | Agents Pôles accueil physique et téléphonique | | |
| R14 | Réglementations applicables | Données à caractère personnel (si oui, voir également R15 à R18)  Réglementations financières & comptables  Précisez : | | |
| R15 | Données à caractère personnel (DCP) | Avis du CIL demandé  Avis du CIL obtenu  Avis du CIL non nécessaire | | |
| R16 | DCP : moyens de collecte | Fichier interne/externe  Requête  Questionnaire  Précisez : | | |
| R17 | DCP : information des personnes | Sur le questionnaire  Journal interne  Sur site web  Autres : Affichage | | |
| R18 | DCP : estimation de la population concernée | Régime général  Population française  Si autre, nombre estimé : | | |

R19 : décrivez brièvement le projet, sa finalité, ses contraintes.

|  |
| --- |
| L'applicatif permet de déclarer un incident entre un agent d'accueil et un client. Selon un mode opératoire précis, il informe certains cadres et agents de directions. La seconde phase enregistre la réponse de la CPAM face à la situation. Un module de statistiques donne la possibilité de requêter sur le type d'incident et les accueils les plus concernés. |

R20 : Classifiez[[2]](#footnote-2) en quatre niveaux les informations saisies ou traitées dans le système.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Niveau* | *Informations traitées* | *Origine*  *(base, organisme…)* | *Destinataire*  *(base, organisme…)* | *Durée de conservation* |
| Secret |  |  |  |  |
| Confidentiel | Date de l'incident  Agent d'accueil concerné  Lieu  Nature du public  Nature des incivilités  Motif  Déroulement (peut contenir le NIR et le nom-prénom de l’assuré) | CPAM | Agents d'accueil  Encadrement du Pôle  Direction Générale  Service Conditions de travail  Direction des Ressources Humaines  Médecine du Travail | 36 mois |
| Restreint | Suivi des actions  Statistiques | CPAM | Encadrement du Pôle  Direction  Service Conditions de travail  Direction des Ressources Humaines  Médecine du Travail | 36 mois |
| Publique |  |  |  |  |

R21 : Listez les acteurs (ou les rôles) dans le traitement, et leurs droits d’accès sur les niveaux d’informations du système ? (*Aucun accès* ***Ø****; accès en* ***L****ecture uniquement ; accès en lecture et* ***É****criture.*)

| *Acteurs ou rôles* | *Catégories d’informations* | | | |
| --- | --- | --- | --- | --- |
| *Secret* | *Confidentiel* | *Restreint* | *Publique* |
| Agents d'accueil | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. |
| Encadrement du pôle accueil | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. |
| Direction | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. |
| Service Conditions de travail | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. |
| Direction des Ressources Humaines | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. |
| Medecine du travail | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. | Ø  L.  É. |

R22 : Énumérez par ordre chronologique les principales fonctions du processus de traitement.

|  |  |  |
| --- | --- | --- |
| *N°* | *Etapes* | *Principales actions ou fonctions du processus à protéger* |
| 1 | Saisie | Saisie d'un incident par un agent d'accueil |
| 2 | Information | Envoi d'un courriel automatique à DG, DRC, SCT, SDRH, PAP, medecine du travail |
| 3 | Gestion | Selon gravité, saisie par encadrement de l'accueil de la réponse apportée |
| 4 | Saisine de la DRC | Selon la gravité, saisine de la direction pour réponse à apportée |
| 5 | Retour vers l'agent | Information de la décision à l'agent |
| 6 | Classement | Classement du dossier et archivage |

R23 : Indiquez où se procurer la documentation du projet (références documentaires, liens) et le schéma du processus :

Répertoire du projet

R24 : Autres informations utiles à la compréhension du système que conçoit le projet :

Néant

# Risque lié à une divulgation

|  |  |  |  |
| --- | --- | --- | --- |
| **Échelle d’impact** | | | |
| 4 stratégique | 3 critique | 2 sensible | 1 impact faible ou négligeable |

Evaluez les conséquences d’une divulgation accidentelle ou intentionnelle de l’information, dans le pire des cas.

Tableau : Conséquences d'une divulgation

|  | **Types d’impact** | **Évènements redoutés** | **Impact**  (0 à 4) | **Commentaires** |
| --- | --- | --- | --- | --- |
| C1 | Image | La divulgation porte atteinte à la crédibilité de l’organisation auprès de ses clients et partenaires. |  | Les faits rapportés seront purement objectifs |
| C2 | Fraude | La divulgation permet d’exploiter financièrement une faille du système d’information. | 0 | Pas de lien avec les système de paiement des prestations |
| C3 | Surcoûts | La divulgation entraîne une dépense financière (remise aux normes, pénalités). | 0 | Sans objet |
| C4 | Responsabilité légale | La divulgation est en contradiction avec la loi, un règlement ou un contrat. | 2 | Secret professionnel et respect de la loi CNIL |
| C5 | Conséquences pour le personnel | La divulgation porte atteinte au bien-être ou à la motivation du personnel. |  | Perte de confiance dans l’outil |

C6 Commentaire de la MOA :

Néant

# Audit, besoin de preuves et de traces

|  |  |  |  |
| --- | --- | --- | --- |
| **Échelle d’impact** | | | |
| 4 stratégique | 3 critique | 2 sensible | 1 impact faible ou négligeable |

Évaluez les conséquences d’une absence de preuves du bon fonctionnement du système, dans le pire des cas.

Tableau : Analyse du besoin de preuve

|  | **Types d’impact** | **Évènements redoutés** | **Impact**  (0 à 4) | **Commentaires** |
| --- | --- | --- | --- | --- |
| P1 | Contentieux, fraudes | L’absence de preuves issues du fonctionnement du système empêche la recherche des responsabilités. | 0 | Sans objet |
| P2 | Fraude interne, reniement d’action, absence de journalisation du fonctionnement | La modification accidentelle ou délibérée des preuves du fonctionnement du système a des conséquences légales, financières ou sur le fonctionnement du système. | 1 | Trace de la déclaration par l’agent |
| P3 | Responsabilité légale | La divulgation des traces ou preuves peut porter atteinte à l’organisation. | 0 | Sans objet |

P4 Commentaire de la MOA :

Néant

# Risque lié à une perte d’intégrité

|  |  |  |  |
| --- | --- | --- | --- |
| **Échelle d’impact** | | | |
| 4 stratégique | 3 critique | 2 sensible | 1 impact faible ou négligeable |

Évaluez les conséquences d’erreurs dans l’information ou de modifications malveillantes visant à tromper les utilisateurs, dans le pire des cas.

Tableau : Conséquences d'une perte d'intégrité

|  | **Types d’impact** | **Évènements redoutés** | **Impact**  (0 à 4) | **Commentaires** |
| --- | --- | --- | --- | --- |
| I1 | Erreurs de gestion | Des modifications non autorisées de l’information entraînent des décisions de gestion erronées. |  | Incidence sur la réponse à l’incivilité |
| I2 | Perte de traitements en cours | Des modifications non autorisées de l’information entraînent l’interruption ou l’annulation de traitements en cours (liquidation, avis, instructions, etc.) |  | Non réponse à l’incivilité |
| I3 | Fraude | Des modifications non autorisées de l’information peuvent être exploitée par une fraude. | 0 | Sans objet |
| I4 | Confiance du public | Les erreurs ou les modifications non autorisées d’information portent atteinte à l’image publique ou la réputation de l’Assurance maladie auprès de ses clients, partenaires et fournisseurs. | 0 | Sans objet |
| I5 | Surcoûts | Les erreurs ou les modifications non autorisées de l’information entraînent des surcoûts - par exemple pour rechercher les erreurs et reconstruire l’intégrité d’informations perdues ou corrompues. |  | Temps de ressaisie ou traitement |
| I6 | Responsabilité légale | Les erreurs ou les modifications non autorisées de l’information conduisent au non-respect de dispositions légales, réglementaires ou contractuelles. | 2 | Secret professionnel et respect de la loi CNIL |
| I7 | Conséquences pour le personnel | Les erreurs ou les modifications non autorisées de l’information ont un impact sur la confiance du personnel dans le système - par exemple les utilisateurs ne se fient pas au système et organisent des solutions de remplacement. |  | Perte de confiance dans l’outil |

I8 Commentaire de la MOA :

Néant

# Risque lié à une perte de disponibilité

|  |  |  |  |
| --- | --- | --- | --- |
| **Échelle d’impact** | | | |
| 4 stratégique | 3 critique | 2 sensible | 1 impact faible ou négligeable |

Évaluez les conséquences de l’arrêt prolongé du système, dans le pire des cas, et précisez dans quel délai ces conséquences deviendraient insupportables.

Tableau : Conséquences d'une perte de disponibilité

|  | **Types d’impact** | **Évènements redoutés** | **Impact** | Délai de réalisation | | | | | **Commentaires** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| < 4h | < 24h | 2 à 5 jours | 1 à 4 semaines | >= 1 mois |
| D1 | Décisions de pilotage | L’arrêt du fonctionnement nuit à des décisions de gestion. |  |  |  |  |  |  | Pas de notion d'urgence – retour possible en solution papier |
| D2 | Perte de traitements en cours | L’arrêt du fonctionnement affecte des traitements en cours (liquidation, avis, etc.) |  |  |  |  |  |  | Solution alternative possible |
| D3 | Fraude | L’arrêt du fonctionnement peut être exploité par une fraude. | 0 |  |  |  |  |  | Sans objet |
| D4 | Confiance du public | L’arrêt du fonctionnement porte atteinte à l’image publique ou la réputation de l’Assurance maladie auprès de ses clients, partenaires et fournisseurs. | 0 |  |  |  |  |  | Usage uniquement interne |
| D5 | Surcoûts | L’arrêt prolongé du système entraîne des surcoûts. |  |  |  |  |  |  | Temps de traitement en solution alternative |
| D6 | Responsabilité légale | L’arrêt de fonctionnement conduit au non-respect de dispositions légales, réglementaires ou contractuelles. | 0 |  |  |  |  |  | Sans objet |
| D7 | Conséquences pour le personnel | L’arrêt de fonctionnement a un impact sur le bien-être ou la motivation du personnel. |  |  |  |  |  |  | Relais possible par papier |
| D8 | Variations du besoin de disponibilité dans le temps | A quel moment le besoin de disponibilité est-il maximum? |  | Permanent  période : | | | | | Besoin quotidien |
| D9 | Reconstruction, après redémarrage, des données non traitées | Une fois le système redémarré, faudra t-il reconstruire les données entrantes qui n’auraient pas été traitées pendant l’interruption ? | non |  | | | | |  |
| D10 | Reconstruction, avant redémarrage, des données non traitées | Faudra t-il, avant de redémarrer, reconstruire au préalable les données entrantes non traitées pendant l’interruption ? | non |  | | | | |  |
| D11 | Délai impératif de reconstruction (si « oui » à D9 ou D10 | Dans quel délai devra t-on reconstruire l’information non traitée pendant l’interruption ? | 0 |  |  |  |  |  | Sans objet |

D12 Commentaire de la MOA :

Néant

# Evaluation SSI (réservée au MSSI)

|  |  |
| --- | --- |
| Direction | Pierre ROUSSEAU, Directeur général de la CPAM 44 |
| Application ou projet | Gestion des Incidents avec le Public |
| Date | 21/11/16 Enr.24/11/16 - Impr.09/02/12 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Échelle d’impact** |  |  |  | **Analyste des risques SSI** |
| 4 | stratégique | 2 | sensible |  | Nom/service : Ayroulet Nadège \_ MSSI Cellule SSI |
| 3 | critique | 1 | faible ou négligeable |  | Téléphone : 02.51.88.89.92 |

|  |
| --- |
| *Avis technique impossible / analyse non réalisée / nécessité d’informations complémentaires* |

Tableau : Evaluation du système à partir des informations fournies par la maîtrise d’ouvrage

| **Le risque global** pour la sécurité de l’information est le suivant : **D1** **; I2 ; C2** **; P1**  Commentaire :  Le risque global de ce projet est évalué à 2 (sensible), en raison d’un besoin de protection des données nominatives relevant du champ de la CNIL et d’un besoin d’intégrité des informations renseignées. |
| --- |

Tableau : Recommandations en l’état des informations transmises

| **Préconisations** |
| --- |
| **L’analyse est suffisante pour exprimer les besoins de sécurité**  Les principaux objectifs de sécurité à atteindre sont :  Confidentialité Les données nominatives dans l’application relèvent du champ de la CNIL et du respect du secret professionnel.  Intégrité Des modifications non autorisées pourraient avoir des incidences sur la réponse aux incivilités.  Disponibilité Un dysfonctionnement de l’application entrainerait un retour au formulaire papier.  Preuves et fraudes Le risque est faible mais un besoin de preuve peut être nécessaire, pour la CPAM (historique des actions réalisées par les agents). |
| **L’analyse doit être approfondie pour pouvoir exprimer les besoins de sécurité**  et en particulier, il est recommandé de :  mener une analyse EBIOS (DCS)  prévoir un audit avant ouverture  prévoir un audit après l’ouverture  organiser une instance de suivi de la sécurité  mener l’action suivante : |

Tableau : demandes du MSSI

| **Demandes transmises ou à transmettre au directeur de projet** | | |
| --- | --- | --- |
| Demande de transmission des documents projet | Oui | Non |
| Demande d’intégrer l’analyste sécurité à la liste de diffusion des comptes-rendus des réunions du projet | Oui | Non |
| Demande de rendez-vous (date      ) | Oui | Non |

Commentaire du MSSI :

Cette application est un outil de déclaration en ligne d’incident entre un agent d’accueil et un client, outil utilisé en interne de la CPAM.

Les mécanismes techniques doivent garantir la confidentialité, l’intégrité et la disponibilité des données traitées dans l’application.

L’accès à l’application doit être protégé et limité aux agents ayant le besoin d’en connaître.

Un mécanisme de traçabilité doit être prévu (historique des actions réalisées par les agents).

# Préconisations techniques (réservé à la maîtrise d’œuvre)

*La section 7 peut ne pas être renseignée si une analyse approfondie a été demandée en section 6*

|  |  |  |  |
| --- | --- | --- | --- |
|  | Nom/service | | Téléphone |
| Intervenant |  | |  |
| Date | | Enr.24/11/16 - Impr.13/09/12 | |

Tableau : Principaux moyens de traitement et de protection envisagés

|  |
| --- |
| *Dans le cas où le système relève de la Loi informatique et libertés du 6 janvier 1978 (cf. question R15), les éléments techniques suivants sont requis pour éclairer le Correspondant Informatique et Libertés (CIL).*  *Au-delà de la simple description de moyens, les préconisations de solutions doivent répondre aux enjeux de la CNIL : l’usage anormal ou illégitime, la modification non souhaitée et la disparition des données à caractère personnel, ainsi que l’impossibilité ou l’erreur dans l’exercice du droit d’accès et de rectification.*  *Les solutions doivent considérer tous les supports du système : matériel, logiciel, transferts, papiers, personnes.*  **T1 Identification et authentification**  Carte agent  Profils d’habilitation SY\_GIP  Login et mot de passe  Autres ou précisions :  **T2 Echanges de données**  En interne :  Liaison informatique (messagerie, serveurs, …)  Support physique (CD, DVD, clef USB, …)  Autres ou précisions :  En externe :  Liaison informatique (messagerie, serveurs, …)  Support physique (CD, DVD, clef USB, …)  Autres ou précisions : Pas d'échange externe  **T3 Journalisation**  Identifiant du poste de travail  Identifiant de l’utilisateur  Date/heure de connexion Date/heure de déconnexion  Opération effectuée en : Consultation Création Mise à jour Suppression Autre  Référence des données accédées  Autres ou précisions : Toutes les actions utilisateurs sont journalisées  **T4 Hébergement des données**  Interne à l’Assurance maladie Externe à l’Assurance maladie  Précisez : |
|  |

T5 Description des solutions, par la MOE :

Application web php hébergée sur serveur Linux, avec base de données MySql version 5, accès sécurisé à la base de données par login/mot de passe.

# Observations du CIL

|  |  |  |
| --- | --- | --- |
|  | Nom/service | Téléphone |
| CIL |  |  |

Ce chapitre est à renseigner par le Correspondant Informatique et Liberté (CIL) de l’organisme.

Tableau : Prise en compte des enjeux CNIL

|  | **Centres d’intérêt CNIL** | **Niveau** | **Commentaires** |
| --- | --- | --- | --- |
| L1 | Caractère identifiant des données traitées | Aucun  Faible  Fort |  |
| L2 | Préjudice potentiel pour les personnes identifiées | Aucun  Faible  Fort |  |
| L3 | Maîtrise du droit d’accès des personnes identifiées aux données les concernant | Insuffisant  Satisfaisant |  |

Tableau : Préconisations du CIL

|  |  |
| --- | --- |
| **L4 Formalités préalables** | **L5 Recommandations** |
| Aucune    Inscription au registre    Demande d’avis    Demande d’autorisation    Présentation d’un projet de Décret en Conseil d’Etat par le Ministère | Nature de la recommandation :  Finalités  Données  Durée de conservation  Sécurités  Information des instances représentatives du personnel |

L6 Commentaire du CIL :

# Guide de remplissage

Objectif du QERSI

Le QERSI analyse les risques qu’un système fait porter au système d’information. Le système étudié peut être une application nouvelle, l’évolution d’une application ancienne, ou une organisation humaine.

Tout projet d’un système modifiant le traitement d’un flux d’information doit bénéficier d’une analyse formalisée qui informe le responsable du traitement sur les risques et les moyens pour y répondre. Le QERSI est réputé connu du responsable du traitement, par sa maîtrise d’ouvrage.

La conduite de la démarche de sécurité est de la responsabilité de la maîtrise d’ouvrage. Le chef de projet de la maîtrise d’ouvrage remplit de manière exhaustive les sections 1 à 5, et joint tout document utile à la compréhension du système à analyser.

Le Manager de la sécurité du système d’information (MSSI) rend son évaluation dans la sixième section du QERSI. Il estime si l’analyse limitée du QERSI est suffisante pour éliminer des risques majeurs, et il répond en formulant des objectifs de sécurité à la maîtrise d’ouvrage, qu’elle transmettra à la maîtrise d’œuvre pour implémentation.

Dans le cas où la sensibilité du projet engage des risques majeurs, il est obligatoire de poursuivre par une analyse complète conforme à l’ISO 27005.

Enfin, le document sera adressé au Correspondant Informatique et Libertés afin qu’il fasse des préconisations sur le projet (section huit).

Démarche de la sécurité dans les projets

L’analyse de risques doit être réalisée en amont des spécifications du cahier des charges, à la phase d’expression des besoins, dès que les informations et les fonctions traitées par le futur système sont connues.

Elle permet notamment :

1- d’estimer l’importance du risque pour le système d’information dans au moins trois critères de sécurité : disponibilité, intégrité, confidentialité.

2- d’identifier les points faibles du système au regard des menaces mises en évidence

3- d’élaborer les mesures de sécurité permettant d’amener le risque à un niveau acceptable

4- d’informer le responsable du projet des risques résiduels

Échelle d’estimation des risques utilisée dans le questionnaire

L’importance du risque pour l’Assurance maladie est exprimée dans une échelle allant de 1 (pas d’impact ou négligeable) à 4 (impact intolérable). La réponse doit être fournie en envisageant le pire des scénarios.

| **Impact** | **Valeur** | **Signification** |
| --- | --- | --- |
| Critique | **4** | Les impacts ne seront pas surmontés ou le risque est inacceptable |
| Important | **3** | Les impacts seront difficilement surmontés |
| Limité | **2** | Les impacts seront surmontés, mais engendreront des difficultés |
| Négligeable | **1** | Les impacts seront surmontés sans difficultés |

Description du questionnaire

Le questionnaire contient huit sections. Les cinq premières sont à remplir par le chef du projet, la sixième est réservée au MSSI, la septième à la maîtrise d’œuvre, la huitième au CIL.

**Section 1 - Profil du projet :** cette section permet de décrire le futur système et son contexte réglementaire, humain et stratégique. Cette description permet d’estimer les moyens organisationnels, techniques et juridiques à mettre en œuvre pour la sécurité. Il est souhaitable d’associer un schéma du processus.

**Section 2 - Divulgation :** cette section couvre les dommages inhérents à une fuite d’information accidentelle ou volontaire (perte de confidentialité) aboutissant à une plainte ou une révélation publique.

**Section 3 - Preuve :** cette section permet de décrire un besoin particulier de preuve pour le projet. En l’absence de besoin spécifique décrit par le chef de projet, ce critère sera étudié par le MSSI en fonction des réponses apportées dans les autres sections.

**Section 4 - Intégrité :** cette section analyse les conséquences de la perte ou de la modification de l’information traitée ou produite par le système, c'est-à-dire : dans quelle mesure ces évènements peuvent tromper l’utilisateur et nuire au processus métier.

**Section 5 - Disponibilité :** cette section estime les dommages consécutifs à l’interruption du fonctionnement de l’application ou du système. Chaque question propose un choix de cinq durées d’arrêt. Il s’agit d’estimer l’impact le plus important, puis de désigner la durée à partir de laquelle l’impact devient inéluctable.

Les questions D9 à D11 concernent la continuité d’activité, au sens de la nécessité de reconstruire les informations qui n’auraient pas pu être traitées pendant l’arrêt du système.

**Section 6 - Réservée à l’estimation du risque par le MSSI :** cette section permet à l’analyste de sécurité de faire une première évaluation de la sensibilité du projet, à la lecture des réponses du chef de projet apportées dans les sections précédentes. Il s’agit d’une appréciation d’expert, qui peut donc diverger par rapport à l’expression de la maîtrise d’ouvrage.

**Section 7 – Observations de la maîtrise d’oeuvre :** cette section recueille les préconisations techniques de la maîtrise d’œuvre, au regard des sections précédentes.

**Section 8 – Observations du Correspondant Informatique et Libertés :** dans la dernière section, le CIL donne son avis sur la prise en compte des enjeux de la CNIL, et fait des préconisations sur les formalités adéquates pour le projet.

*Pour toute question sur ce formulaire, vous pouvez contacter le MSSI de votre organisme.*

Glossaire

|  |  |
| --- | --- |
| *Disponibilité* : propriété qu’une information ou un système soit accessible en temps voulu | *Menace* : acte ou événement pouvant entraîner un impact négatif sur le système d’information ou à l’activité supportée par celui-ci. |
| *Intégrité* : propriété d’assurer l'exactitude de l’information. | *Risque* : description d'un scénario de menace et des pertes auxquels il peut aboutir. |
| *Confidentialité* : propriété que l'information ne soit pas accessible aux individus, entités ou processus non autorisés. |  |
| *Preuve* : propriété de pouvoir imputer sans équivoque les actions d’une personne ou entité. | *Données à caractère personnel :* information permettant l’identification d’une personne physique de manière directe ou indirecte. |

**Echelle de classification des informations pour la confidentialité**

|  |
| --- |
| ***Avertissement***  *L’échelle de classification ci-dessous, conforme à la Politique Ministérielle de sécurité des systèmes d’information, permet d’estimer le besoin de confidentialité d’une information. Des exemples illustratifs sont proposés. Cependant la finalité, l’étendue du projet, sa durée, le nombre d’utilisateur, la population concernée, le volume ou encore l’attractivité particulière des données sont autant de critères qui peuvent modifier le besoin de confidentialité d’une information dans le contexte particulier d’un projet.* |

Tableau : Echelle de classification des informations pour la confidentialité

|  | **Niveau** | **Libellé** | **Exemples** |
| --- | --- | --- | --- |
|  | **4** | **Secret** | **Informations nominatives :**  - Informations de santé : pathologie, antécédents familiaux, observation médicale,  - situations ou comportements à risques  - Informations relatives aux infractions, condamnations ou mesures de sûreté (infractions, condamnations, mesures de sécurité)  - Informations relatives à des suspicions de fraudes ou d’infractions  - Origines raciales ou ethniques, opinions politiques, philosophiques, religieuses, appartenances syndicales des personnes, la vie sexuelle |
| **Informations non nominatives :**  - Informations liées à l’organisation et à la stratégie de l’organisme, dont la révélation aurait un impact critique sur la conduite de ses missions  - Informations liées aux mécanismes de fraudes et aux failles ou vulnérabilités de sécurité, dont la révélation pourrait être exploitée pour nuire aux missions de l’organisme |
|  | **3** | **Confidentiel** | **Toute information nominative ne rentrant pas dans la classe « secret »** et notamment :  - NIR, Etat-civil, identité, données d’identification (nom, prénom, adresse, photographie, date, lieu de naissance),  - Appréciation sur les difficultés sociales des personnes  - Informations d’ordre économique et financière (revenus, situation financière)  - Vie personnelle : habitude de vie, situation familiale et sociale  - Vie professionnelle : CV, Situation professionnelle, Scolarité, formation, Distinction  - Informations biométriques : contour de la main, empreintes digitales, réseaux veineux, iris de l’œil, reconnaissance faciale, reconnaissance vocale, autre procédé |
|  | **2** | **Restreint** | - Données de localisation (déplacement, données GPS, GSM, etc) par satellite, par téléphone mobile ou autre  (adresse IP, logs, etc)  - Identifiants des terminaux, Identifiants de connexions, Information d’horodatage…  - procédures, description de processus, instructions, Intranet  - enregistrements non nominatifs (dates, heures, actions, états, etc.)  - informations personnelles que le salarié a identifiées explicitement comme tel dans le système d’information - Données de connexion |
|  | **1** | **Publique** | Informations ayant vocation à être publiées : éditoriaux, publication Extranet, statistiques publiables, campagnes de communication, etc. |

**Exemples de solutions en fonction de la classification de l’information à protéger**

Les moyens de protection de l’information sont proportionnels à la vraisemblance du risque tel que perçu par le responsable du traitement. Ces protections traitent l’accès, le transfert, le stockage et déterminent la trace utile laissée par l’utilisateur. Les exemples ci-dessous illustrent l’effort de protection en fonction du niveau de confidentialité, dans une liste non exhaustive et dont la pertinence doit être étudiée dans chaque projet.

Tableau : Exemples de solutions habituellement utilisées pour la protection des informations (2011)

|  | **Niveau** | **Libellé** | **Recommandations** |
| --- | --- | --- | --- |
|  | **4** | **Secret** | Contrôle d’accès par authentification forte  Diffusion à une population restreinte dont la liste est tenue à jour  Contrôle de pertinence de la demande d’accès (rebond)  Trace détaillée des accès et des actions, y compris consultation  Protection éventuelle par chiffrement de l’information et du transfert |
|  | **3** | **Confidentiel** | Contrôle d’accès par identification et mot de passe renforcé[[3]](#footnote-3)  Liste des profils ayant un droit d’accès  Gestion des habilitations répondant aux bonnes pratiques  Trace des accès et des actions entraînant un risque  Protection du moyen de transfert |
|  | **2** | **Restreint** | Contrôle d’accès par identification et mot de passe  Liste des domaines ayant un droit d’accès  Trace des accès |
|  | **1** | **Publique** | Pas de besoin de contrôle d’accès |

**Abréviations utilisées dans le document**

AM : Assurance maladie

MOA : maîtrise d’ouvrage

MOE : maîtrise d’œuvre

MSSI : manager de la sécurité du système d’information

CIL : correspondant informatique et libertés

DCP : données à caractère personnel

DCS : dossier central de sécurité basé sur une analyse approfondie de type EBIOS

EBIOS : évaluation des besoins et identification des objectifs de sécurité (méthode de l’ANSSI)

DICP : disponibilité, intégrité, confidentialité, preuve

|  |
| --- |
| *CNAMTS DDO DOCQ DCMOA - Formulaire QERSI – version 2.0 du 18 octobre 2011*  *Pour toutes questions sur ce document, prenez contact avec le MSSI de votre organisme* |

1. Le Directeur de projet est le responsable opérationnel de la conduite du projet, pour le compte du Responsable du traitement. [↑](#footnote-ref-1)
2. Se reporter à l’échelle de confidentialité de l’Assurance maladie en page 11. [↑](#footnote-ref-2)
3. Dans l’Assurance maladie, l’authentification forte par carte agent est la solution par défaut. [↑](#footnote-ref-3)