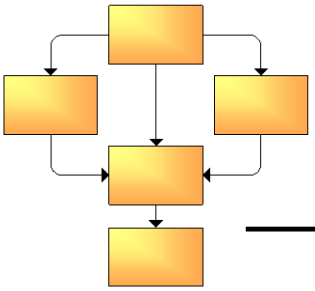


Club EBIOS

Études de cas

Médecine du travail

Date	:	29 novembre 2011
Statut	:	Approuvé
Classification	:	Public
Nombre de pages	:	10
Responsable des travaux	:	Matthieu GRALL
Validation	:	Groupe de travail
Approbation	:	Conseil d'administration

Club EBIOS, 72 avenue Gaston Boissier, 78220 VIROFLAY

Origine du document

Ce document a été réalisé par le Club EBIOS.

Responsable des travaux :

- CNIL (Matthieu GRALL)

Contributeurs :

- ANSSI (Raphaël GUÉRAND, Claire POTUS)
- BULL SAS (Dominique CASTAN, Ludovic LECOMTE)
- CNAM-TS (Stéphane BADACH)
- CONIX (Sylvain CONCHON)
- OPEN (Jean-Jacques BUREAU)
- Cyril PATRIGEON
- Gurvan QUENET

Sommaire

Avertissement

Ce document présente les résultats de l'étude d'un cas fictif, réalisée à titre illustratif.

Il a pour vocation de montrer qu'il est possible d'étudier des risques sur la vie privée à l'aide de la méthode EBIOS. Elle ne doit donc pas être utilisée en l'état pour des cas similaires au cas étudié.

On note qu'une étude réelle et complète demande généralement plus de détails et d'explications, notamment pour garantir l'exhaustivité de l'étude des menaces et pour démontrer que les risques appréciés sont suffisamment traités par les mesures choisies.

Introduction

Ce document présente une étude de cas de l'utilisation de la méthode EBIOS pour gérer des risques sur la vie privée de personnes concernées par un traitement de données à caractère personnel.

Le contexte est un petit cabinet de médecine du travail d'une entreprise française d'environ 400 employés. Le traitement étudié consiste à gérer les dossiers de médecine du travail de ses employés. L'étude des risques a pour objectif d'améliorer la protection de la vie privée des employés.

Que se passerait-il si les données de santé d'un employé étaient altérées à son insu ?
Quid du droit d'accès à son dossier médical après avoir été déclaré inapte par son employeur ?
Et si la presse faisait écho de l'aggravation de l'état de santé d'un des dirigeants de l'entreprise ?

1 Contexte : la gestion de dossiers de médecine du travail

L'étude a tout d'abord consisté à identifier ce que l'on souhaite sécuriser : les « éléments à protéger ». Il s'agit des données à caractère personnel dont la compromission, la modification ou la disparition entraînerait un préjudice pour les personnes concernées, et des processus légaux qui leur permettent notamment d'exercer leurs droits. Le contexte du fonctionnement normal est également analysé. Ce sont les lois, règlements et procédures que doivent respecter les utilisateurs du système.

Le traitement a pour finalité de gérer les dossiers de médecine du travail des employés de l'entreprise. Il permet à l'équipe de médecine du travail (professionnels de santé) :

- ✓ d'accéder et de mettre à jour les dossiers médicaux des employés ;
- ✓ de produire des documents administratifs (en particulier la fiche d'aptitude) ;
- ✓ de garder trace des passages à l'infirmerie (notion de registre ou de main courante) ;
- ✓ de réaliser des enquêtes avec production de résultats agrégés.

Concernant les processus légaux, les employés sont tout d'abord informés oralement de leurs droits lors de leur première visite.
Ils peuvent ensuite exercer leurs droits (accès, rectification…) auprès de leur service des ressources humaines s'agissant des données administratives. Pour les données médicales, le Code de la santé publique prévoit la demande directe de l'employé au médecin sur toutes ses données de santé[1], avec des exceptions réglementées (cas psychiatriques ou incurables, présence ou non d'un tiers médecin pour révéler l'information).
Dans le cas d'un employé déclaré inapte et désirant avoir accès aux informations qui ont conduit à la décision, l'employé demande transmission des informations à un médecin qu'il désigne (ou un expert désigné par le magistrat sur la liste homologuée), et celui-ci rend son avis qui est versé aux pièces du débat contradictoire.

Les données à caractère personnel se décomposent en :

- ✓ des données d'identification des employés au sein de l'entreprise (identité, poste de travail...) ;
- ✓ des données de santé les concernant (antécédents médicaux, examens médicaux, informations cliniques et paracliniques collectées lors des bilans programmés et consultations inopinées, détermination de l'aptitude, conseils de prévention donnés...).

Elles sont couvertes par le secret professionnel, et certaines par le secret médical.

Mesures existantes identifiées
Les données sont stockées dans une base de données sur le disque dur chiffré du serveur. Celles-ci sont sauvegardées intégralement chaque semaine et de manière incrémentale chaque jour, sur des disques durs chiffrés, stockés dans une armoire forte ignifugée. Une procédure prévoit de prévenir immédiatement les employés en cas de violation de leurs données à caractère personnel.

[1] Toute personne a accès à l'ensemble des informations concernant sa santé détenues par des professionnels et établissements de santé. (Art. L. 1111-7)

On note que dans ce cadre, les principales références réglementaires à respecter sont les suivantes :

- ✓ le [Rapport-2004] ;
- ✓ la [Loi-I&L] : les données d'identification et celles qui décrivent l'individu (ici sa santé et sa carrière) constituent ce que la CNIL nomme les données à caractère personnel. Elles relèvent d'une réglementation particulière qui devra être prise en compte ;
- ✓ les [Reco-ANAES] ;
- ✓ le [Décret-Confid] ;
- ✓ le Code pénal ;
- ✓ le Code de la santé publique, et le Code de déontologie médical qu'il contient.

Les supports ont également été identifiés. Leurs caractéristiques peuvent comporter des vulnérabilités qui peuvent être exploitées pour que des menaces se concrétisent.
Le cabinet est composé d'une assistante médicale qualifiée, d'une infirmière diplômée d'État, d'un médecin inscrit à l'Ordre et d'un informaticien chargé de l'administration et de la maintenance. L'infirmière et le médecin font systématiquement un point avant chaque consultation et une réunion d'organisation et de gestion du planning a lieu tous les mois.
Physiquement, le cabinet est composé de quatre salles : une salle d'attente dans laquelle on trouve le bureau de l'assistante, une salle pour l'infirmière, un cabinet de consultation pour le médecin et un petit local informatique fermé à clé.
Les membres du cabinet manipulent de nombreux documents papier (fiche de liaison prévue par le code du travail, fiche d'identification administrative et professionnelle du salarié, historique des postes, exposition à des risques et périodes d'exposition, fiches d'examens complémentaires…).
La gestion des dossiers des employés et les processus légaux reposent sur un système informatique autonome, séparé du système de l'entreprise et non connecté à Internet. Ce système comprend un serveur (avec un système d'exploitation courant) et des postes de travail (avec un système d'exploitation courant, un logiciel métier, une suite bureautique et un client lourd de messagerie) reliés par un réseau local filaire. Un pont vers le réseau de l'entreprise permet d'accéder à la messagerie électronique. Le logiciel métier (DRTRAVAIL) permet de couvrir l'ensemble des activités du cabinet, de produire des documents administratifs, de gérer les rendez-vous et de conserver la mémoire des examens médicaux réalisés. On note enfin que le cabinet dispose d'un réseau téléphonique fonctionnant en ToIP (*Telephony over Internet Protocol*).

Mesures existantes identifiées
Les logiciels sont mis à jour lors des interventions de l'administrateur informatique ou du support bureautique.

Les sources de risques ont enfin été identifiées. Ce sont ces sources qui peuvent être à l'origine des menaces. Dans le contexte étudié, les plus plausibles sont les suivantes :

- ✓ un code malveillant d'origine inconnue (virus, vers, logiciel espion…) introduit par accident ;
- ✓ une compagnie d'assurance qui convoiterait les données des employés ;
- ✓ l'employeur qui chercherait à connaître l'état de santé d'un employé absent, ou à détruire des données d'un employé victime d'une maladie professionnelle ou d'un accident du travail ;
- ✓ un employé (pour faire pression sur un cadre en menaçant de divulguer son état de santé) ;
- ✓ un pirate informatique qui chercherait de l'information sur une personne en particulier ou viserait à démontrer la négligence de l'entreprise ;
- ✓ un concurrent qui chercherait à déstabiliser l'entreprise ;
- ✓ le personnel médical qui pourrait provoquer un incident de manière accidentelle, ou agir par curiosité mal placée ;
- ✓ l'administrateur informatique, le support bureautique ou le personnel d'entretien, qui pourrait être soudoyé pour voler des données sur des dirigeants de l'entreprise ;
- ✓ des incidents ou sinistres accidentels (panne de courant, dégât des eaux, incendie…).

Mesures existantes identifiées
L'accès physique est contrôlé par un personnel toujours présent à l'accueil et les locaux sont fermés à clé. L'accès au système informatique est contrôlé à l'aide d'un identifiant et d'un mot de passe non trivial. Les droits associés à chaque compte utilisateur se limitent aux seules actions qu'ils ont à réaliser. Un logiciel antivirus est installé et mis à jour à chaque intervention de l'administrateur informatique. Il faut également signaler que les professionnels de santé sont bien sensibilisés à la déontologie et à la protection du secret des informations médicales.

2 Les risques : violations de données de santé et menaces liées aux personnes autorisées

L'étude a ensuite consisté à déterminer les risques à partir des éléments précédemment identifiés qui les composent, et à les estimer en termes de gravité et de vraisemblance, compte tenu des mesures existantes. Le tableau suivant présente les résultats de l'appréciation des risques[2] :

Événements redoutés et impacts les plus graves[3]	Gravité	Justifications	Menaces les plus vraisemblables	Vraisemblance maximale	Justification
Accès illégitime aux données[4] : l'image et la réputation des employés pourraient être atteintes (maladie mentale, maladie sexuellement transmissible…), ainsi que leur vie privée (lieu de vie confidentiel, relation extraconjugale…)	4. Maximal	- Le caractère identifiant est jugé maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant. - Le caractère préjudiciable est jugé important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés. - Les mesures existantes ne permettent pas de réduire la gravité.	- Les utilisateurs légitimes (professionnels de santé, administrateur informatique et support bureautique) pouvant accéder aux données non chiffrées pourraient, de manière accidentelle ou délibérée (s'ils sont soudoyés), détourner l'usage du système d'exploitation, du système de gestion de la base de données, du logiciel métier ou des logiciels de bureautique (fouille de contenu, croisement illégitime de données…). - Ils pourraient modifier ces logiciels (piégeage par un *keylogger* logiciel…). - Ils pourraient transférer des données sur des clés USB non chiffrées. - Une personne (salarié de l'entreprise, pirate informatique, compagnie d'assurance, concurrent…) pourrait tenter de voler des documents papier ou de récupérer des supports papier	3. Important	- Les vulnérabilités des supports sont jugés importantes : il semble possible de réaliser les menaces en s'appuyant sur les caractéristiques des supports. - Les capacités des sources de risques sont jugées importantes : les sources de risques ont des capacités réelles, jugées comme élevées, pour réaliser les menaces. - Bien que les données soient stockées sur un disque chiffré, cela ne permet pas d'empêcher les personnes ayant accès au disque d'accéder aux données. Les mesures de sécurité physique réduisent légèrement les vulnérabilités des supports et capacités des sources de risques.

[2] On note que seuls les risques dont la gravité est élevée ou très élevée ont fait l'objet d'une étude de menaces.

[3] On ne considère que les impacts qui portent sur les libertés et la vie privée des personnes concernées, et non ceux qui portent sur l'organisme.

[4] Par des tiers non autorisés.

Événements redoutés et impacts les plus graves[3]	Gravité	Justifications	Menaces les plus vraisemblables	Vraisemblance maximale	Justification
			ou électroniques mis au rebut. - Une compagnie d'assurance ou un concurrent pourrait voler des matériels (postes de travail, disques durs externes, serveur…) ou payer quelqu'un pour le faire.		
Modification non désirée des données : le statut d'aptitude des employés pourrait être faussé avec toutes les conséquences possibles sur leur carrière et leur intégrité physique (licenciement, mauvais suivi des risques de santé, voire invalidité ou décès…)	4. Maximal	- Le caractère identifiant est jugé maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant. - Le caractère préjudiciable des impacts est jugé maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter. - Les sauvegardes permettraient de récupérer les données mais pas de détecter une altération.	- Les utilisateurs légitimes pourraient détourner l'usage des logiciels (modifications dans une base de données…). - Ils pourraient les modifier (contagion par un code malveillant, manipulation inopportune lors de la mise à jour, configuration ou maintenance, substitution d'un composant par un autre…).	3. Important	- Les vulnérabilités des supports sont jugées importantes : il semble possible de réaliser les menaces en s'appuyant sur les caractéristiques des supports. - Les capacités des sources sont jugées importantes : les sources de risques ont des capacités réelles, jugées comme élevées, pour réaliser les menaces. - Les mesures de sécurité logique et physique réduisent quelque peu les vulnérabilités des supports et les capacités des sources de risques.
Modification du traitement : les employés pourraient perdre la maîtrise de leurs données.	3. Important	- Le caractère identifiant est jugé maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant. - Le caractère préjudiciable des impacts est jugé limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés. - Les mesures existantes ne permettent pas de réduire la gravité.	- Le personnel médical pourrait détourner l'usage des logiciels (modifications dans une base de données…). - L'administrateur pourrait les modifier (évolution des fonctionnalités, manipulation inopportune lors de la mise à jour, configuration ou maintenance, substitution d'un composant par un autre…).	1. Négligeable	- Les vulnérabilités des supports sont jugées importantes : il semble possible de réaliser les menaces en s'appuyant sur les caractéristiques des supports. - Les capacités des sources de risques sont jugées négligeables : les sources de risques ne semblent pas avoir de capacités particulières pour réaliser la menace.
Disparition des	2. Limité	- Le caractère identifiant est jugé			

Événements redoutés et impacts les plus graves[3]	Gravité	Justifications	Menaces les plus vraisemblables	Vraisemblance maximale	Justification
données : les employés pourraient être pris en charge de manière non adaptée ou se retrouver dans l'incapacité de faire valoir leurs droits.		maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant. - Le caractère préjudiciable est jugé important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés. - Les sauvegardes et la réaction prévue en cas de violation des données permettent de contenir significativement les conséquences d'une disparition de données.			
Indisponibilité des processus légaux[5] : les employés pourraient ne pas connaître les raisons de leurs statut d'aptitude, ne pas pouvoir apporter des éléments complémentaires ou rectificatifs…	2. Limité	- Le caractère identifiant est jugé maximal : il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant. - Le caractère préjudiciable des impacts est jugé limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés. - Les sauvegardes et la réaction prévue en cas de violation des données permettent de contenir significativement les conséquences d'une indisponibilité des processus.			

Une cartographie a été réalisée pour les risques dont la gravité est élevée et très élevée (voir le schéma en fin d'étude).

[5] C'est-à-dire si les employés n'étaient pas informés, s'ils ne pouvaient pas avoir accès à leurs données après avoir été déclarés inaptes, les rectifier, etc. On note que l'organisme s'expose à des poursuites pénales pour non respect de la [Loi-I&L].

3 Les mesures : l'amélioration du dispositif de sécurité

Les risques d'accès illégitime aux données à caractère personnel, de modification non désirée et de modification du traitement doivent absolument être évités ou réduits. Afin de les réduire à un niveau acceptable, des mesures complémentaires doivent être déterminées et mises en œuvre.

Quant aux autres risques, l'application de bonnes pratiques doit permettre d'améliorer la manière dont ils sont traités. On note qu'ils devraient également être réduits par l'application des mesures destinées à traiter les autres risques.

Une mesure radicale consiste à **anonymiser les données d'identification des personnes concernées au niveau de la base de données ou de l'application**, en plus du chiffrement du disque où elles sont stockées, afin de les rendre inintelligibles pour quiconque ayant un accès direct au serveur. Cette anonymisation doit évidemment être réversible pour les utilisateurs autorisés.
Une mesure organisationnelle consiste à réduire le nombre de techniciens autorisés à intervenir sur le système, à formaliser leur habilitation et tracer leurs actions (date, heure, motif d'intervention). Le contrat de maintenance devra prévoir une clause de confidentialité.
Cela contribue fortement à réduire la vraisemblance du risque lié à l'accès illégitime aux données.

Il convient également de **formaliser les habilitations** en appliquant les principes du moindre privilège et du besoin d'en connaître (ex : l'assistante médicale accède aux données sous la responsabilité du médecin mais n'a pas nécessairement besoin d'accéder à l'ensemble du dossier), et de **mettre en place une identification et authentification** des membres du cabinet. La solution la plus efficace est d'employer la carte de professionnel de santé (CPS). Cette solution pourrait également permettre la signature électronique des documents et des courriers électroniques, et le chiffrement de fichiers. À défaut, l'utilisation d'un mot de passe à usage unique (solution OTP[6] transmettant un mot de passe par SMS sur le téléphone portable du membre du cabinet en faisant la demande avec un code PIN) peut être envisagée. Dans un premier temps, il est possible de continuer à procéder au déverrouillage des postes avec un mot de passe, dans la mesure où la politique de mots de passe est renforcée[7].
Ces mesures contribuent à diminuer la vraisemblance de tous les risques en diminuant les capacités des sources de risques.

Par ailleurs, **la traçabilité doit être sérieusement gérée**. Ainsi, les connexions au système depuis les postes de travail devront être journalisées et horodatées, de même que les requêtes effectuées et leur résultat. Tous les journaux seront exportés vers un serveur dédié, conservés six mois et des mesures assurant leur intégrité devront être mises en place. Ces journaux devront être régulièrement inspectés, éventuellement au moyen d'outil d'analyse automatique, afin de détecter d'éventuelles opérations non désirées.
Ceci contribue à réduire la vraisemblance de tous les risques en agissant notamment sur le sentiment d'impunité des sources de risques.

D'autres mesures devraient compléter le dispositif :

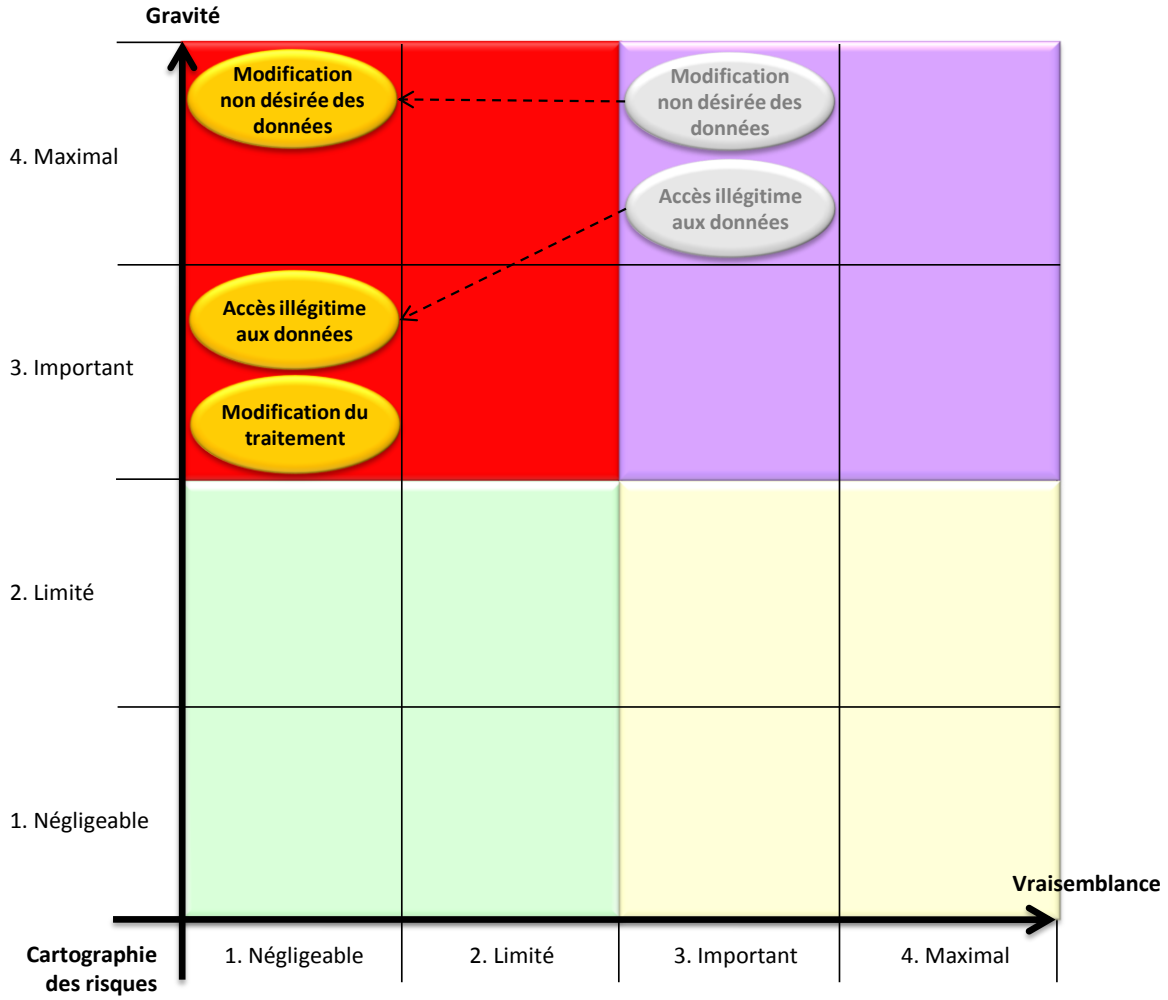
- ✓ sensibiliser les membres du cabinet aux risques, aux mesures à appliquer et aux sanctions prévues en cas de manquement ;
- ✓ afficher une procédure d'accompagnement des visiteurs ou des intervenants de maintenance ;
- ✓ formaliser les procédures détaillées correspondant aux processus légaux (par exemple sous la forme d'une brochure explicative, fournie lors de leur première visite, et affichée dans le cabinet), et les appliquer de manière systématique, pour réduire la vraisemblance d'une impossibilité d'exercer ses droits ;
- ✓ améliorer la maîtrise des supports externes (clé USB, disques durs externes…) en prévoyant de n'autoriser que ceux prévus à cet effet, pour réduire encore la vraisemblance des risques ;
- ✓ mettre en œuvre une procédure pour la mise au rebut des supports papier et électronique à l'aide d'un outil d'effacement sécurisé et d'un broyeur approprié, pour réduire la vraisemblance d'un accès illégitime ;

[6] *One Time Password*.

[7] Voir les bonnes pratiques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : http://www.securite-informatique.gouv.fr/gp_article45.html.

- ✓ stocker les sauvegardes chiffrées dans un lieu distinct et sécurisé, pour réduire la gravité d'une modification ou d'une disparition de données et la vraisemblance d'un accès illégitime ;
- ✓ formaliser une procédure utilisable en cas de violation de données, pour réduire la gravité de tous les risques ;
- ✓ compléter les clauses des contrats de maintenance informatique (interdiction de l'échange standard des disques défectueux, de l'externalisation des sauvegardes…).

Les risques sont ré-estimés en tenant compte de ces mesures, afin d'évaluer les risques résiduels :



On constate que la gravité des risques reste importante, bien que ces événements puissent être contenus ou récupérés, car ils restent grandement préjudiciables pour les personnes concernées. Pour diminuer encore la gravité, il aurait fallu, par exemple, collecter moins de données ou empêcher la survenance des impacts, ce qui n'a pas été jugé possible.

Conclusion

Cette étude de cas montre que la méthode EBIOS peut être employée très simplement pour étudier les risques sur la vie privée.

Annexes

Acronymes

CNIL	Commission Nationale de l'Informatique et des Libertés
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité

Glossaire

Donnée à caractère personnel	Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [Loi-I&L]
Traitement de données à caractère personnel (traitement)	Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. [Loi-I&L]

Bibliographie

Les références suivantes apparaissent entre crochets dans le présent document.

[Loi-I&L]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[8].
[Décret-Confid]	Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique.
[Rapport-2004]	*Le dossier médical en médecine du travail*, Rapport du Conseil national de l'Ordre des médecins, 2004.
[Reco-ANAES]	Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès (recommandations de l'ANAES – Agence Nationale d'Accréditation et d'Évaluation en Santé).
[EBIOS]	*Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques*, 25 janvier 2010, ANSSI.

[8] Modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.