Commission Nationale de l'Informatique et des Libertés

Sécurisation des données de santé au travail

14 novembre 2013
Matinée d'étude du CISME

Marc-André BEAUDET
Ingénieur IT, Service de l'expertise
mbeaudet@cnil.fr

Mickaël TOME
Juriste, Service des Affaires Juridiques
mtome@cnil.fr

Plan

I. Cadre juridique

- La CNIL: statut, composition, missions
- Présentation de la loi du 6 janvier 1978 modifiée
- Champ d'application de la loi
- Conditions de licéité des traitements
- L'utilisation encadrée des données de santé
- Les formalités à accomplir auprès de la CNIL

II. Principales mesures de sécurité

- Mesures de sécurité physiques et logiques
- Politique d'habilitation forte
- Authentification forte
- Traçabilités des actions
- Pérennité des données
- Confidentialité des données stockées et transmises
- Charte informatique

III. Mesures complémentaires

- Cas des hébergeurs de données de santé
- Fonctions de CIL et de RSSI
- Architecture sécurisée du système d'information
- Analyse de risque et PSSI

I. Cadre juridique

Cadre juridique

La CNIL: statut et composition

- Une autorité administrative indépendante composée de 17 membres (hauts magistrats, parlementaires, conseillers économiques et sociaux, personnalités qualifiées)
- Une présidente élue par ses pairs: Isabelle Falque-Pierrotin
- Les membres de la CNIL ne reçoivent d'instruction d'aucune autorité.
- Budget de 13 millions d'euros, services: 160 personnes

Cadre juridique

Les missions de la CNIL

- **Informer** et conseiller les autorités, les professionnels et le grand public (site internet, guides, permanence téléphonique…) ;

- **Recenser** les traitements déclarés : le « fichier des fichiers » ;

- **Contrôler** l'application de la loi au sein des organismes ;

- **Sanctionner** en cas de non-respect de la loi ;

- **Réglementer** (normes simplifiées, autorisations uniques, recommandations…) ;

- **Garantir le droit d'accès** indirect aux traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique (fichiers STIC, JUDEX, RG…).

Cadre juridique

Présentation de la loi du 6 janvier 1978 modifiée

- **La loi n 78-17 du 6 janvier 1978**
  - Une éthique de l'informatique appliquée aux données personnelles (art. 1er LIL)
- **La refonte de la loi « Informatique et Libertés » par la loi du 6 août 2004**
  - Une mise à jour (directive européenne 95/46/CE, évolutions technologiques)
  - Allègement des formalités déclaratives
  - Des pouvoirs de contrôle accrus (la santé au programme des contrôles 2011-12)
  - Des pouvoirs de sanction accrus (avertissement, mise en demeure, sanction pécuniaire)
  - L'institution des Correspondants Informatique et Libertés
  - Délivrance de labels et renforcement de la veille prospective
- **Vers l'adoption d'un règlement européen de protection des données personnelles**

Cadre juridique

Le champ d'application de la loi Informatique et Libertés (1/3)

- **La donnée à caractère personnel (art. 2 LIL)**

  - Toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement par référence à un numéro d'identification (ex: n de sécurité sociale) ou un ou plusieurs éléments qui lui sont propres (ex: initiales du nom et du prénom, date de naissance + commune de résidence, biométries…)

  - Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens d'identification dont dispose le responsable du traitement ou toute autre personne (ex: tables de correspondance)

  - La prise en compte par la loi des méthodes d'anonymisation des données (suivi épidémiologique du SIDA, codage des accès pour l'assurance maladie complémentaire, PMSI, SNIIRAM)

Cadre juridique

Le champ d'application de la loi Informatique et Libertés (2/3)

- **Le fichier/traitement de données à caractère personnel (art. 2 LIL)**

  - Traitement: toute opération ou tout ensemble d'opérations portant sur de telles données, quelque soit le procédé utilisé (ex: collecte, enregistrement, organisation, conservation, modification, extraction, consultation, utilisation, communication, rapprochement, interconnexion, verrouillage, effacement, destruction (*bases de données, applications cartes à puce, sites web, transferts de fichiers sur internet…*)

  - Fichier: tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés

Cadre juridique

Le champ d'application de la loi Informatique et Libertés (3/3)

- **Le responsable de traitement (art. 3 LIL)**

  - **Critère de détermination**: la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens, sauf désignation expresse par les dispositions législatives ou réglementaires relatives au traitement

  - **Lieu d'établissement**: responsable établi sur le territoire français (installation stable, quelle que soit sa forme juridique, filiale, succursale…) ou qui recourt à des moyens de traitement situés sur le territoire français (article 5 LIL)

Cadre juridique

Les conditions de licéité des traitements de données personnelles

- Une **finalité** déterminée, explicite et légitime
- Des **données** adéquates, **pertinentes**, non excessives et mises à jour
- Une **durée de conservation limitée** des données : la consécration d'un droit à l'oubli
- Des mesures de **sécurité** adaptées: confidentialité, intégrité et pérennité des données
- Le respect des **droits des patients**
  - Droit à l'information du patient (art. 32 LIL)
  - Droit d'accès aux données personnelles
  - Droit d'opposition pour des raisons légitimes (discrétionnaire, consentement parfois)

Cadre juridique

L'utilisation très encadrée des données de santé (1/2)

- **La reconnaissance dans la loi du caractère « sensible » des données de santé**

  - Un principe d'interdiction de traitement (article 8 LIL)

« Il est interdit […] de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celui-ci ».

Cadre juridique

L'utilisation très encadrée des données de santé (2/2)

- **Des <u>exceptions</u> qui permettent le traitement des données de santé:**

  - Le **consentement exprès** de la personne, sauf dans le cas où la loi prévoit qu'il ne suffit pas

  - Les traitements mis en œuvre par des médecins ou des biologistes aux fins de la **médecine préventive**, des **diagnostics médicaux**, de l'**administration des soins** ou de traitements

  - La **recherche médicale**

  - L'**intérêt public**

  - Les traitements de données qui font l'objet **à bref délai** d'un procédé d'**anonymisation**

  - Les traitements d'**évaluation des pratiques de soins**

Cadre juridique

Les formalités à accomplir devant la CNIL (1/3)

- **La déclaration**

- Le régime de droit commun: la **déclaration normale**

  - Ex: les fichiers de gestion administrative et médicale des hôpitaux, services de santé, services de médecine préventive

- La **déclaration simplifiée** pour les traitements les plus courants et sans danger manifeste

  - Ex: normes simplifiées pour les fichiers des cabinets médicaux et para-médicaux (50), les pharmacies (52), les laboratoires (53) les opticiens (54)

Cadre juridique

Les formalités à accomplir devant la CNIL (2/3)

- **La demande d'avis**
  - Saisine de ministères portant sur des projets de textes
  - Saisine d'organismes du secteur public portant sur des projets d'acte réglementaire
  - Traitements de l'État intéressant la sûreté, la défense, ou la sécurité publique
  - Traitements de l'État ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales
  - Téléservices de l'administration électronique
  - Certains traitements comportant le NIR ou des données biométriques

Cadre juridique

Les formalités à accomplir devant la CNIL (3/3)

- **La demande d'autorisation**

  - Pour le secteur privé, seront soumis à autorisation les traitements portant sur:
    - des **données sensibles**,
    - des **données génétiques**,
    - des données relatives aux **infractions, condamnations et mesures de sûreté**,
    - ceux susceptibles d'exclure du **bénéfice d'un droit**, d'une prestation ou d'un contrat,
    - ceux ayant pour objet l'**interconnexion** de fichiers correspondant à des intérêts publics ou finalités différents
    - Ceux comportant le **N.I.R.** (art. 25-I-6)
    - Ceux comportant des appréciations sur les **difficultés sociales** des personnes
    - Ceux portant sur les **données biométriques** nécessaires au contrôle d'identité des personnes

Cadre juridique

Les formalités à accomplir devant la CNIL - Santé

- **Les cas spécifiques d'autorisations dans le domaine de la santé**
  - Le régime de l'autorisation « Recherche » (chap. IX LIL)
  - Le régime de l'autorisation « Evaluation de pratiques de soins » (chap. X LIL)
  - Le régime de l'autorisation « Anonymisation à bref délai » (art. 8-III et 25 LIL)
  - Le régime de l'autorisation « Intérêt public » (art. 8-IV et 25 LIL)
  - Le régime de l'autorisation « Transferts hors Union européenne » (art. 68 et s. LIL)

II. Principales mesures de sécurité

Principales mesures de sécurité

Notion de sécurité d'un système d'information

- **La confidentialité,**
- **L'intégrité**
- **La disponibilité**

- D'autres aspects peuvent être pris en compte: la non répudiation, la gestion de la preuve (traçabilité notamment), l'authentification, …

Principales mesures de sécurité

Mesures de sécurité physiques

- Les mesures de sécurité physiques permettent de contrôler l'accès physique aux données:
  - Contrôle d'accès: badge, biométrie (soumis à autorisation), …
  - Vidéosurveillance (soumis à autorisation ou déclaration),
  - Protection incendie,
  - Climatisation,
  - Liaison dédiée,
  - Redondance de salle serveur,
  - Gardiennage
  - …

Principales mesures de sécurité

Mesures de sécurité logiques

- Les mesures de sécurité logiques permettent de contrôler l'accès aux données via un système d'information:

  - Confidentialité: gestion des accès (politique d'habilitation, authentification), chiffrement, cloisonnement des réseaux, …

  - Intégrité: journalisation, calcul d'empreintes numériques, redondance des journaux, chiffrement, somme de contrôle,

  - Disponibilité: sauvegarde, archivage, cluster d'application, virtualisation de services, redondance réseau, …

Principales mesures de sécurité

Politique d'habilitation forte

- Il est nécessaire de mettre en œuvre une politique de gestion des habilitations afin de n'autoriser l'accès aux données de santé qu'aux personnes qui ont le besoin d'en connaître,

- Cette politique d'habilitation doit :
  - être revue régulièrement,
  - être intégrée dans les circuits arrivée/départ et changement de poste d'un employé,
  - être définie selon des profils et des missions,
  - être basée sur le principe du moindre privilège

Principales mesures de sécurité

Authentification forte

- Différence entre identification et authentification:
  - Identification: je dis qui je suis
  - Authentification: je prouve que je suis bien la personne que je dis être

- Authentification:
  - Par ce que l'on est, que l'on fait (*eg* biométrie),
  - Par ce que l'on sait (*eg* mot de passe),
  - Par ce que l'on a (*eg* carte à puce)

Principales mesures de sécurité

Authentification forte

- Authentification basique vs authentification forte:
  - Authentification basique: utilisation d'un seul vecteur,
  - Authentification forte: utilisation d'au moins 2 vecteurs différents,

- Authentification forte via la carte CPS pour les professionnels de santé

Principales mesures de sécurité

Traçabilité des actions

- Toutes les actions relatives aux accès en lecture, écriture, modification et suppression doivent êtres tracées: **traces fonctionnelles**

- Des traces du système doivent être également générées (arrêt des traces, blocage d'un compte, modification de droits, accès aux données du système, …): **traces techniques**

- Toutes ces traces doivent faire l'objet d'une revue régulière afin de détecter toute action suspecte, elles ne doivent être accessibles que par un nombre limité de personnes (typiquement, l'équipe sécurité ou le RSSI)

- Des mesures techniques peuvent permettre d'assurer leur intégrité (système WORM: Write Once Read Many, centralisation des journaux, calcul d'empreintes, …)

Principales mesures de sécurité

Pérennité des données

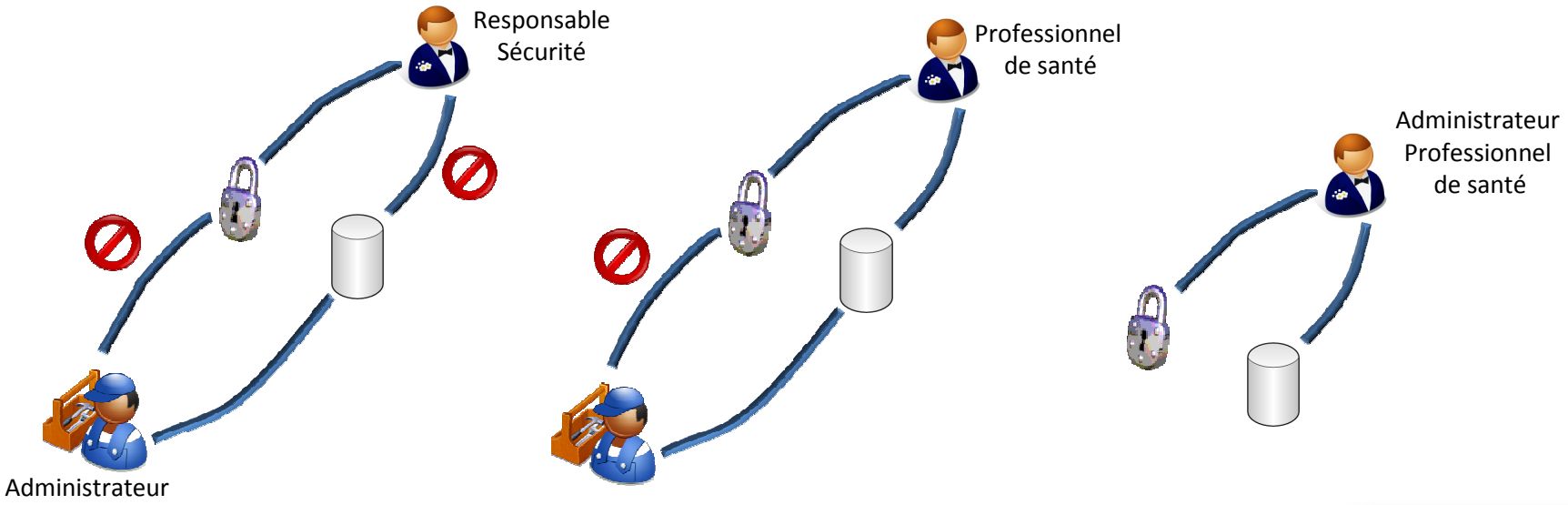
■ Des sauvegardes doivent être régulièrement appliquées afin d'assurer une disponibilité des données, elles doivent *a minima* suivre les recommandations suivantes:

- Stockage dans un local sécurisé et éloigné du lieu de production,
- Dans le cadre d'une sauvegarde en ligne, la transmission doit être sécurisée
- Effacement des supports de sauvegardes de manière sécurisée avant recyclage,
- Chiffrement des données sauvegardées
- Politique de sauvegarde réfléchie et adaptée aux contraintes métier
- Régulièrement testées dans le cadre d'un Plan de Reprise d'Activité (PRA)

Principales mesures de sécurité

Confidentialité des données stockées vis-à-vis des administrateurs: chiffrement

- L'administrateur n'est pas habilité à accéder aux données de santé, sauf si c'est un professionnel de santé (il n'en a pas le besoin d'en connaître),
- Il doit toutefois pouvoir accéder à l'ensemble des plateformes pour les administrer et les maintenir,
- Une solution: les données stockées doivent être chiffrées avec une clé dont il n'a pas connaissance, détenue par une personne qui elle n'a pas accès aux données.



Principales mesures de sécurité

Confidentialité des données stockées vis-à-vis des administrateurs

Cas particulier d'un problème technique sur une donnée de santé

- Exemple de cas particuliers: un médecin de prévention utilise une application métier fournie par un prestataire. Lors de l'enregistrement d'une donnée de santé, l'opération échoue. Il doit donc faire intervenir sont prestataire.

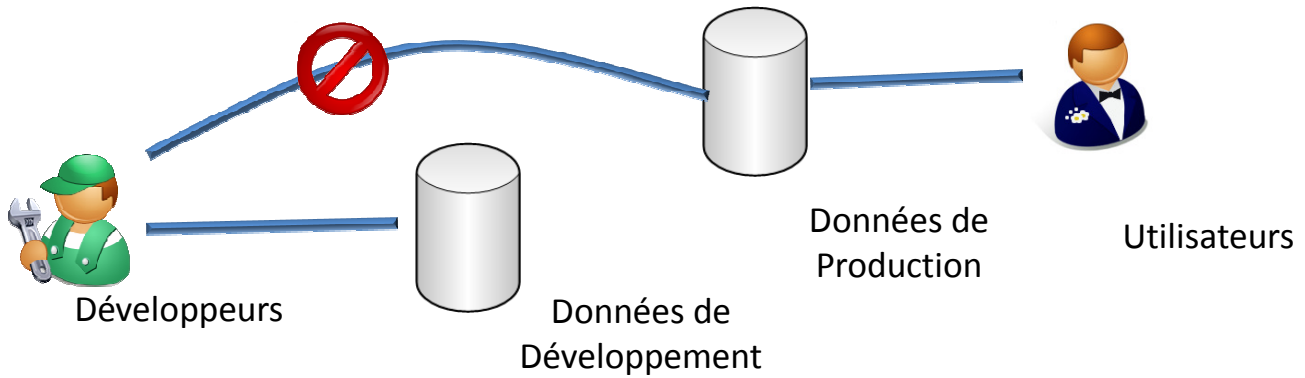
- Une procédure stricte doit être mise en œuvre:

1. L'accès par défaut ne doit être possible (idéalement, une mesure technique l'interdit),
2. Une autorisation spécifique et préalable d'un professionnel de santé de l'organisme (en l'occurrence, le médecin de prévention) est donnée,
3. Le prestataire accède à la donnée et effectue son opération de maintenance,
4. Il informe l'organisme de la fin de la tâche d'administration, la mesure technique est de nouveau posée,
5. Le prestataire envoie un rapport à l'organisme en précisant notamment le nom du professionnel de santé ayant autorisé l'accès, le détail de l'autorisation spécifique, la liste des actions effectuées avec un horodatage précis.

Principales mesures de sécurité

Confidentialité des données stockées vis-à-vis des développeurs: chiffrement

- Les développeurs d'une application métier hébergeant des données de santé doivent être en mesure de tester leur application,
- Ces tests ne doivent pas porter sur des données de production (extraction d'une base, jeu de sauvegarde, …)
- Seul un jeu de test peut être utilisé.



Principales mesures de sécurité

Charte informatique

- L'utilisation d'un système d'information dans la sphère professionnelle doit être encadrée, une charte informatique, présentée préalablement à tout accès à ce système d'information, permet de définir les règles d'utilisation.

- Elle doit prévoir principalement:
  - Un rappel du contexte, de l'environnement de travail et des règles de protection des données,
  - Les modalités d'utilisation du système d'information,
  - Les modalités d'intervention du personnel technique et leurs prérogatives,
  - Les sanctions encourues en cas de non respect de cette charte.

III. Mesures complémentaires

Mesures complémentaires

Cas des hébergeurs de données de santé

- L'externalisation des données de santé auprès d'un organisme tiers, distinct du professionnel ou de l'établissement de santé qui fournit aux patients concernés des activités de prévention, de diagnostic ou de soins est soumis à une procédure d'agrément (art. L1111-8 du code de la santé publique)

- Cet agrément[1] est délivré par le ministre en charge de la santé, après avis du Comité d'Agrément des Hébergeurs (dont l'ASIP Santé assure le secrétariat). La CNIL est également saisie pour avis sur les demandes d'agrément.

- Les agréments sont délivrés quand des mesures très exigeantes de sécurité sont mises en œuvre par le candidat (authentification forte, traçabilité, chiffrement, pérennité des données).

- L'agrément est délivré pour une durée de 3 ans et pour un service spécifique.

(1) http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

Mesures complémentaires

Fonction de CIL[1]

- Objet: accompagnement pédagogique, diffusion de la culture « Informatique et Libertés »

- Avantages:
  - Dispense de la plupart des déclarations (mise en place d'un registre),
  - Relation privilégiée avec la CNIL (service dédié, intranet, …)
  - Formations délivrées par la CNIL

- Statut:
  - Interne ou externe,
  - Indépendant dans cette mission,
  - En lien direct avec la direction afin d'apporter conseils et alertes nécessaires au niveau stratégique
  - La responsabilité du responsable de traitement n'est pas reportée sur le CIL en cas de manquement

- Profil: juriste, informaticien, auditeur

(1) Pour aller plus loin: http://www.cnil.fr/linstitution/missions/informer-conseiller/correspondants/

Mesures complémentaires

Fonction de RSSI

- Objet: Personne en charge de la définition et de l'application d'une politique de sécurité du système d'information spécifique à un organisme

- Avantages:
  - Spécialiste en charge des enjeux stratégiques du système d'information
  - Permet à la DSI de se consacrer exclusivement aux aspects fonctionnels

- Statut (recommandations):
  - Interne ou externe (attention cependant à la sensibilité des données),
  - Indépendant dans cette mission,
  - En lien direct avec la direction afin d'apporter conseils et alertes nécessaires au niveau stratégique

- Profil: informaticien, auditeur

Mesures complémentaires

Architecture sécurisée

- Un système d'information peut être pensé dès sa création de manière sécurisée (security by design).

- Une sécurité absolue n'est pas atteignable, mais l'application de plusieurs mesures vis-à-vis d'un même risque permet de réduire de manière significative les compromissions éventuelles: concept de défense en profondeur.

- De très nombreuses fonctionnalités permettent de sécuriser un système d'information: cloisonnement réseau, chiffrement, filtrage, détection et prévention d'intrusion, redondance, load balancing, cluster, système d'exploitation spécifique, proxy, reverse proxy, honeypot, …

Mesures complémentaires

Analyse de risques

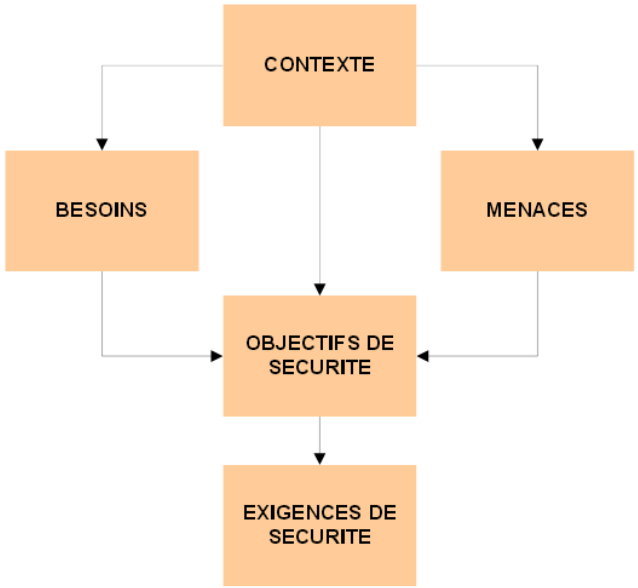
- Afin de définir les mesures de sécurité spécifiques à un traitement, une analyse de risques doit être menée. Elle consiste en une liste objective des risques encourus et des mesures permettant de les réduire ou les annuler.

- Plusieurs méthodes peuvent être utilisées: Mehari (CLUSIF), Marion (CLUSIF), EBIOS (ANSSI), chapitre 4 de la norme ISO 27002, …

- Le résultat d'une analyse de risques permet de définir les mesures (techniques et organisationnelles) à mettre en œuvre pour répondre aux objectifs de sécurité de l'organisme. Ce résultat est l'élément d'entrée d'une Politique de Sécurité du Système d'Information, PSSI.

Mesures complémentaires

Analyse de risques: exemple de la méthode EBIOS



Méthode EBIOS

1. Vision globale et explicite du système étudié, des enjeux, des contraintes et référentiels applicables: CONTEXTE

2. Définition des éléments à protéger en terme de disponibilité, intégrité et confidentialité et mise en évidence des impacts en cas de sinistre: BESOINS

3. Recensement des scénarios pouvant porter atteinte aux composants du SI: MENACES

4. Mise en évidence des risques réels et expression de la volonté des les traiter en cohérence avec le contexte particulier de l'organisme : OBJECTIFS DE SECURITE

5. Spécification des mesures concrètes à mettre en œuvre pour traiter les risques sur la base d'une négociation argumentée.: EXIGENCE DE SECURITE

Mesures complémentaires

PSSI

- Les mesures définies en sortie de l'analyse de risque doivent être formalisées dans un document type: une Politique de Sécurité des Systèmes d'Information

- Ce document doit être le plus exhaustif possible, il doit couvrir les aspects organisationnels et techniques. (sécurité réseau, sécurité des serveurs, sécurité des liaisons, sécurité des postes nomades, …)

- Il ne définit pas forcément les mesures précises (qui peuvent présentées dans une PSSI Opérationnelle).

- Tout comme l'analyse de risque, ce document doit être revu régulièrement afin de s'assurer qu'il est en adéquation avec les contraintes réelles.

Merci pour votre attention

Liens utiles:

Guide « Professionnels de santé »
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_professionnels_de_sante.pdf

La sécurité des données personnelles
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/index.html

Méthode pour gérer les risques sur les libertés et la vie privée
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf

Catalogue de mesures pour traiter les risques de la vie privée
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf