Caisse Nationale de l'Assurance Maladie

des Travailleurs Salariés **Sécurité Sociale**

Circulaire CNAMTS

Date :
26/11/91

Origine :
DGA

Mmes et MM les Directeurs
des Caisses Primaires d'Assurance Maladie
des Caisses Générales de Sécurité Sociale
des Caisses Régionales d'Assurance Maladie
MM les Directeurs des CETELIC
MM les Médecins Conseils Régionaux
M le Médecin Chef de La Réunion
(pour attribution)

Réf. :

DGA n° 8/91

Plan de classement :
113

Objet :
LA SECURITE INFORMATIQUE : LES MOTS DE PASSE.
Ce document fait partie du Guide de la Sécurité Informatique en cours de rédaction par le CESSI.
Déjà diffusé : en décembre 1989, un document sur les aspects juridiques de la Sécurité Informatique, complété en
juillet 1991 par circulaire DGA n° 7/91.

Pièces jointes :

Liens :

Date d'effet : **Date de Réponse :**

Dossier suivi par : CESSI - M VERDAGUER

Téléphone : (16) 61.21.04.11

@

Direction de la Gestion Administrative

	Mmes et MM les Directeurs des Caisses Primaires d'Assurance Maladie
26/11/91	des Caisses Générales de Sécurité Sociale des Caisses Régionales d'Assurance Maladie
Origine :	MM les Directeurs des CETELIC
DGA	MM les Médecins Conseils Régionaux M le Médecin Chef de La Réunion (pour attribution)

N/Réf. : DGA n° 8/91

Objet : Document relatif aux MOTS DE PASSE.

En matière de sécurité, le mot de passe est un des moyens les plus répandus d'identification de personnes ayant accès au système d'information.

Pour que l'objectif poursuivi par l'utilisation des mots de passe soit atteint, il est nécessaire de respecter des règles précises et de prendre un certain nombre de précautions. Cette note vous aidera à choisir les mots de passe, à les mémoriser et, de façon plus générale, à les gérer en respectant les recommandations réglementaires ou techniques qui régissent ce domaine.

Le document relatif aux mots de passe fait partie du Guide de la Sécurité Informatique en cours de rédaction par le C.E.S.S.I.

Il est prévu dans les douze prochains mois la diffusion des notes suivantes :

- VIRUS ET INFECTIONS INFORMATIQUES
- PROTECTION DES INFORMATIONS
- INTEGRITE DES DONNEES
- TECHNIQUES DE CHIFFREMENT ET SECURITE

Il est recommandé d'assurer une large diffusion de ce document ou d'une synthèse de ce document auprès du personnel.

Le C.E.S.S.I. :

1 Place Alfonse Jourdain
31000 TOULOUSE

Tél. : 61.21.04.11

se tient à votre disposition pour tout complément d'information.

Le Directeur Délégué

F. POISNEUF

Pour consulter les pièces jointes à cette circulaire, vous pouvez télécharger celles-ci sur micro-ordinateur et lire ou éditer les documents SOUS WORD POUR WINDOWS.

DEMIO/DIVISION STRATEGIE PLANIFICATION METHODES

Centre d'Etudes des Sécurités du Système d'Information

SECURITE INFORMATIQUE
NOTE CONCERNANT LES MOTS DE PASSE

Dans cette note

Cette note vous aidera à :

- Choisir des mots de passe
- Créer des mots de passe
- Employer des mots de passe
- Définir les rôles respectifs du responsable de sécurité et de l'utilisateur
- Concevoir des systèmes utilisant des mots de passe
- Connaître la position de la CNIL.

Première diffusion : novembre 1991

TABLE DES MATIERES

- Dictionnaire des mots de passe
- Recommandations de la CNIL sur les mots de passe

I N T R O D U C T I O N

Il y a trois méthodes de base permettant de vérifier l'identité prétendue d'un individu, qui reposent sur la reconnaissance :

- d'un élément connu de l'individu,
- d'un élément possédé par l'individu,
- d'un élément au sujet de cet individu.

Un élément connu de l'individu peut être un mot de passe.

Les mots de passe sont le moyen le plus utilisé. Ils constituent un facteur clé de la sécurité.

1. - GENERALITES SUR LES MOTS DE PASSE

1.1 Définition

Un mot de passe est une suite de caractères utilisée pour authentifier une identité.

Le fait de connaître le mot de passe qui est associé à une IDENTITE UTILISATEUR donne l'autorisation d'utiliser les facultés associées à cette IDENTITE UTILISATEUR.

1.2 Propriétés des mots de passe

Un mot de passe doit être :

- Difficile à deviner
- Facile à retenir
- Changé fréquemment
- Bien protégé

1.3 Vulnérabilité des mots de passe

Les mots de passe sont vulnérables à plusieurs menaces :

- Observation
- Vol
- Recherche heuristique
- Ecoute passive et active
- Dérivation du flux des données

L'utilisateur doit prendre toute mesure utile pour conserver à son mot de passe son caractère personnel et confidentiel.

Il doit pour ce faire s'imposer des règles de sécurité.

1.4 Emploi des mots de passe

L'utilisation des mots de passe obéit à certaines règles :

* *On doit fournir à tout nouvel utilisateur d'un système informatique un mot de passe.*

* *On doit le changer à intervalles réguliers.*

* *Le système doit conserver une base de données sécurisée des mots de passe.*

* *Les utilisateurs doivent retenir leur mot de passe.*

* *Les utilisateurs doivent utiliser les mots de passe pour s'authentifier lorsqu'ils utilisent le système.*

2. - CHOIX DES MOTS DE PASSE

2.1 Mots de passe choisis par l'utilisateur

L'ensemble des études montre que les utilisateurs choisissent spontanément des mots de passe faibles ou très faibles (voir annexe 1).

2.1.1 Création de mots de passe personnels

On ne doit pas utiliser :

Un nom, un prénom, un surnom, un nom de rue, un code départemental, un numéro de Sécurité Sociale, un numéro de téléphone, un numéro d'immatriculation, un acronyme informatique (par exemple : IBM) ou autre (par exemple : CNAM), un mot quelconque que l'on puisse trouver dans un dictionnaire français ou étranger.

Quelques règles de base :

* *On doit utiliser toute la longueur du champ disponible pour le mot de passe (en règle générale : 8 caractères).*

* *Ces huit caractères doivent être une combinaison de lettres, de chiffres et de caractères spéciaux.*

* *Si le système fait la différence entre les minuscules et les majuscules, on doit utiliser les deux types de caractères.*

* *Le mot de passe doit comprendre si possible des caractères spéciaux (&, ?, I...) ou numériques).*

2.1.2 Une méthode (parmi d'autres) pour créer un mot de passe

a) Choisir deux mots sans relation.

b) Choisir un chiffre ou un caractère spécial.

c) Créer le mot de passe en amalgamant :

- *une syllabe du premier mot,*
- *le caractère non alphabétique,*
- *une syllabe du deuxième mot.*

d) Ne pas écrire le mot de passe mais se souvenir de la manière dont on l'a créé.

Exemple : Renard Bruxelles 7 ➔ ard7Brux

Cette méthode n'emploie qu'un seul caractère non alphabétique.

2.1.3 Autres "mots de passe" provenant de l'individu : les mots de passe cognitifs

Dans un tel système l'utilisateur ne s'identifie pas en donnant un mot de passe à proprement parler mais en répondant à 20 questions personnelles.

Des questions portant sur des faits :

- Quel était le nom de votre école primaire ?
- Quel est le nom de votre oncle préféré ?
- Quel était le nom de votre meilleur(e) ami(e) au collège ?

et des questions portant sur des opinions :

- Quelle est votre fleur favorite ?
- Quel est votre légume préféré ?
- Si vous deviez changer de profession, laquelle choisiriez-vous ?

Un système de ce type semble être une alternative crédible aux mots de passe classiques dans des cas où la sécurité l'emporte sur l'ergonomie.

(Pour des données chiffrées, voir annexe 2)

2.2 Mots de passe générés par la machine

2.2.1 Un générateur de mot de passe

Il est relativement facile de créer un mot de passe qui soit difficile à deviner, mais il est plus ardu de faire en sorte qu'il soit facile à retenir. Un des moyens pour réussir cela consiste à générer par ordinateur des mots de passe prononçables (voir annexe 3).

3. PROCEDURE D'EMPLOI DES MOTS DE PASSE

3.1 Obligation pour des systèmes protégés par des mots de passe

Les systèmes à base de mots de passe doivent se conformer aux objectifs suivants (inspirés de l'ouvrage du DOD - Le Ministère de la Défense des Etats-Unis - : Password Management Guideline).

3.1.1 En matière d'identification

Les systèmes employant des mots de passe utilisés pour le contrôle d'accès aux systèmes informatiques traitant des informations classifiées ou sensibles, doivent être capables d'identifier de manière certaine chacun des utilisateurs du système individuellement.

3.1.2 En matière d'authentification

Les systèmes employant des mots de passe utilisés pour le contrôle d'accès aux systèmes informatiques traitant des informations classifiées ou sensibles, doivent permettre l'authentification non équivoque de l'identité prétendue de l'utilisateur.

3.1.3 En matière de secret du mot de passe

Les systèmes employant des mots de passe doivent assurer, dans la mesure du possible, une protection de la base de données des mots de passe cohérente avec la protection accordée aux informations sensibles traitées par le système informatique.

3.1.4 En matière d'audit

Les systèmes employant des mots de passe utilisés pour le contrôle d'accès aux systèmes informatiques qui traitent des informations classifiées ou sensibles, doivent aider à la détection de la dégradation des mots de passe.

3.2 Responsabilités du responsable sécurité du système d'information

3.2.1 Mots de passe fabricant

Bon nombre de systèmes sont livrés avec des mots de passe standards (SYSTEM, TEST, MASTER...). Le responsable sécurité doit changer ces mots de passe.

3.2.2 Mots de passe initiaux

C'est sous la responsabilité du responsable sécurité que sont générés les mots de passe initiaux ; il n'en prend pas connaissance, seul l'utilisateur connaît son mot de passe. Si le mot de passe est généré par ordinateur et s'il est distribué sur papier, il doit être scellé. Si l'utilisateur est présent lors de sa génération, l'organisation des lieux doit être telle que personne d'autre ne puisse le voir, le temps d'affichage doit être réduit au strict minimum.

3.2.3 Changement de mot de passe

Lorsque le mot de passe d'un utilisateur n'est plus sûr ou est oublié, le responsable sécurité doit pouvoir le changer.

3.2.4 Identité de groupe

En aucun cas plusieurs personnes ne peuvent partager un mot de passe identique, même à des moments différents.

3.2.5 Revalorisation de l'identité d'un utilisateur

Le responsable sécurité doit mettre en place une procédure pour mettre fin à la validité des mots de passe correspondant au personnel quittant l'organisme.

D'autre part, une opération de revalidation des identités et des renseignements généraux sur les personnes (adresse, téléphone,...) doit être réalisée au moins une fois par an.

3.3 Responsabilités de l'utilisateur

3.3.1 Avoir connaissance des règles de sécurité

L'utilisateur doit savoir qu'il doit conserver son mot de passe secret et avertir de ses changements de statuts, des violations de sécurité...

On recommande de faire signer à tous les utilisateurs un document par lequel ils certifient avoir pris connaissance de leurs responsabilités en matière de sécurité.

3.3.2 Changement de mot de passe

Les mots de passe doivent être changés à intervalles réguliers de manière à rendre inopérante toute divulgation non détectée. D'autre part, **l'utilisateur doit être en mesure de changer de mot de passe sans que le responsable sécurité n'intervienne**.

3.3.3 Durée de vie d'un mot de passe

Le point faible d'une sécurité bâtie autour de l'utilisation de mots de passe est la divulgation de ces mots de passe. Plus longtemps on utilise un mot de passe donné pour authentifier, plus longtemps il reste exposé. La probabilité de divulgation d'un mot de passe augmente au fur et à mesure de sa durée d'utilisation. On réduit cette vulnérabilité en réduisant la durée de vie du mot de passe.

Quel que soit le mot de passe, il doit avoir une durée de vie maximum d'utilisation. Quel que soit le milieu et les circonstances, un mot de passe ne peut avoir une durée de vie à 1 an.

Un mot de passe doit être invalidé à la fin de sa durée de vie.

3.3.4 Autorisation de changement

Un utilisateur doit pouvoir changer de mot de passe. Au moment du changement, il doit rentrer son mot de passe et son identité.

3.3.5 Procédure de changement

Le changement a lieu lorsque le mot de passe est périmé, ou au moment choisi par l'utilisateur qui doit être informé de la procédure à suivre et doit, d'autre part, s'assurer que personne ne peut le voir.

Le système doit fournir un nouveau mot de passe. L'utilisateur doit le rentrer deux fois de suite de manière à ce que le système puisse s'assurer qu'il est connu et retenu.

3.3.6 Se souvenir des mots de passe

L'utilisateur doit se souvenir de son mot de passe. En aucun cas il ne doit être écrit.

3.4 Mécanisme d'authentification

Le système doit stocker les identités des utilisateurs autorisés ainsi qu'une représentation des mots de passe (les mots de passe chiffrés, le plus souvent par une fonction à sens unique) et si nécessaire les autorisations associées à chacun des utilisateurs.

Ces informations doivent être soumises à un contrôle d'accès, faute de quoi elles pourraient être modifiées de manière illicite.

Les mots de passe stockés dans la base de données doivent être protégés par un dispositif de contrôle d'accès intégré dans le système, par le chiffrement des mots de passe ou par les deux.

Il est impératif d'utiliser le chiffrement, même si le contrôle d'accès est considéré comme suffisant. Le processus de chiffrement doit avoir lieu juste après l'entrée du mot de passe, la portion de mémoire contenant le mot de passe en clair doit être effacée dès que le chiffrement est terminé. D'autre part, seule la forme chiffrée du mot de passe doit être conservée dans le système. La comparaison se fait sur les formes chiffrées des mots de passe et non pas sur les mots de passe en clair.

3.4.1 Entrée du mot de passe

L'utilisateur doit fournir son identité puis son mot de passe. Si le mot de passe est correct, le système doit afficher la date et l'heure du dernier log-in de l'utilisateur.

3.4.2 Transmission

Lors de la transmission d'un mot de passe du terminal de l'utilisateur vers l'ordinateur au niveau duquel l'authentification est faite, le mot de passe doit être protégé de manière cohérente avec les données qu'il protège.

3.4.3 Taux de tentatives de log-in

En fixant le taux de tentatives de log-in, on peut donner une limite aux nombres de tentatives de découverte du mot de passe par un intrus pendant la durée de vie de ce mot de passe.

Le contrôle du taux de découverte des mots de passe doit se faire en fonction des accès au niveau de chacun des ports d'accès de manière à interdire à l'intrus toute possibilité de passer d'un port à l'autre. Si l'intrus se trouve dans la situation où il peut passer d'un port à l'autre, le taux de découverte des mots de passe doit être contrôlé sur une base personnelle.

On conseille un taux maximum de tentatives de log-in compris entre un par seconde et un par minute.

3.4.4 L'audit (document d'audit)

Le système doit pouvoir générer un document d'audit comportant les utilisations et les changements de mots de passe. Ce document ne contient pas les mots de passe en activité ni les mots de passe rejetés à la suite d'erreurs de frappe.

Il comprend les événements suivants :

* *Les log-in réussis*
* *Les log-in avortés*
* *L'utilisation des procédures de changement de mot de passe*
* *Le blocage de l'identité d'un utilisateur lorsque son mot de passe devient périmé*

Pour chacun de ces événements :

* *Le type d'événement*
* *L'heure et la date*
* *L'identité prétendue de l'utilisateur en cas de log-in avorté*
* *L'identité de l'utilisateur dans tous les autres cas*
* *Le lieu de l'événement (par exemple terminale ou port d'accès...)*

Le document d'audit doit, d'autre part, comporter les changements de mots de passe, réussis ou non.

3.4.5 Notification en temps réel au responsable sécurité

Toute tentative de cinq log-in successifs doit être rapportée en temps réel au responsable sécurité ou au responsable système.

3.4.6 Notification à l'utilisateur

Lors d'un log-in réussi, le système donne à l'utilisateur :

* la date et l'heure du dernier log-in de l'utilisateur
* le lieu du dernier log-in,
* toutes les tentatives infructueuses de log-in correspondant à l'identité de l'utilisateur depuis le dernier log-in réussi.

3.5 Protection du mot de passe

3.5.1 Découverte lors de la première tentative

La probabilité d'une découverte lors de la première tentative dépend de la taille du mot de passe et de la distribution des caractères dans cet espace. Etant donné que bon nombre de mots de passe créés par l'utilisateur ne satisfont pas ces conditions, les mots de passe doivent être générés par un algorithme.

3.5.2 Distribution des mots de passe

Lors de la distribution, les mots de passe doivent être protégés de la même manière que les données auxquelles ils donnent accès.

IV - REMARQUES A L'ATTENTION DES CONCEPTEURS

Le mot de passe doit pouvoir être changé par l'utilisateur aussi fréquemment qu'il le désire.

Obligation de rappeler l'ancien avant modification, avec interdiction contrôlée par le logiciel de réutiliser les *n* derniers mots de passe ($n > 5$) et de réutiliser plus de la moitié des caractères constituant le dernier mot de passe.

Le mot de passe doit être changé au moins une fois par mois. Ce changement doit être imposé par le logiciel, ce qui nécessite une date de validité. L'utilisateur doit être informé suffisamment à l'avance de l'échéance du changement, pour éviter des choix trop rapides qui seraient susceptibles de nuire aux caractéristiques ci-dessus développées et d'entraîner des difficultés de mémorisation.

L'affichage du mot de passe sur écran ou sur imprimante doit être invisible.

Le demande du mot de passe doit être faite à chaque connexion. A ce sujet, il est recommandé que l'usager puisse obtenir à cette occasion, un enregistrement lui donnant les caractéristiques de son dernier accès.

Le mot de passe peut être demandé en cours de session (authentification continue).

Prévoir un délai entre chaque essai d'accès infructueux.

Limiter (inférieur à 4) et enregistrer le nombre d'accès infructueux.

4.1 Règles concernant le stockage et le transport

Le stockage du mot de passe doit être effectué sous une forme chiffrée. Il en est de même lorsque le mot de passe doit transiter sur la ligne.

4.2 Unix et les mots de passe

Le système UNIX permet de définir un utilisateur sans obliger à avoir un mot de passe. Le mot peut être modifié :

- Par un utilisateur après contrôle du mot de passe actuel.
- Par un super utilisateur sans contrôle du mot de passe actuel.

Le système n'enregistre pas les modifications des mots de passe. Les mots de passe sont stockés, chiffrés dans le fichier/ETC/PASSWD. Le chiffrement des mots de passe est conçu pour résister aux attaques systématiques. Il est toutefois recommandé de :

- rendre /ETC/PASSWD inaccessible (le champ des mots de passe est crypté),

- supprimer les champs des commentaires dans /ETC/PASSWD (si ce champ existe, il ne doit contenir aucune information permettant de retrouver le mot de passe).

ANNEXES

Annexe 1 : Typologie des mots de passe

Annexe 2 : Les mots de passe cognitifs

Annexe 3 : Générateur de mots de passe

Annexe 4 : Dictionnaire des mots de passe

Annexe 5 : Recommandations de la CNIL. sur les mots de passe

ANNEXE 1 : TYPOLOGIE DES MOTS DE PASSE

Passwords in use in a university timesharing environment
B. Riddle, M. Miron, J. Semo
Computer & Security November 1989 569-579

L'article est basé sur l'analyse de 6226 mots de passe librement choisis par les utilisateurs pour exploiter le système informatique de l'Université de Syracuse aux Etats-Unis.

	Types de mots de passe	**Nombre**	**Pourcentage**
Groupe 1	2 caractères alphabétiques	1	non-significatif
Groupe 2	3 caractères alphabétiques	891	14,30 %
Groupe 3	5 caractères alphabétiques ou plus	1299	20,90 %
Groupe 4	Caractères alphabétiques et chiffres	215	3,50 %
Groupe 5	Mot de passe de 4 caractères alphabétiques employé (involontairement) par plusieurs personnes	158	2,50 %
Groupe 6	Mot de passe de 4 caractères employé par une seule personne	3662	58,80 %
		6226	100,00 %

ANNEXE 2 : LES MOTS DE PASSE COGNITIFS

L'étude réalisée par M. Zviran W. Haga (d'après : Cognitive passwords : the key to easy access control M. Zviran W. Haga Computer & Security december 90 p 723/731), a consisté à faire créer un mot de passe de huit caractères à une population donnée, à fournir à chacun de ses membres un autre mot de passe de huit caractères et à faire répondre à un questionnaire du type défini ci-dessus.

Trois mois plus tard, les personnes étudiées ont été invitées à se souvenir de leurs deux mots de passe et à répondre à nouveau au questionnaire : les taux de réussite sont les suivants :

Mot de passe :

- Personnel : 35 % . 86 % s'en souviennent de mémoire
  . 14 % en l'écrivant

- Fourni : 23 % . 34 % s'en souviennent de mémoire
  . 66 % en l'écrivant

Questionnaire :

Les bonnes réponses varient entre 75 % et 98 %.

La moyenne est de 82 %.

D'autre part, les questionnaires de chaque personne ont été testés sur leur entourage professionnel et familial. Personne n'a pu donner plus de la moitié des réponses correctes et la moyenne s'est élevée à 27 % de réponses correctes.

ANNEXE 3 : GENERATEUR DE MOTS DE PASSE

B. Allberty *(1)* a conçu un programme de ce type en procédant de la sorte :

Le programme utilise un tableau comportant des fragments prononçables, ces fragments sont classifiés en tant que consonnes, voyelles longues et courtes. A chacun des éléments du tableau correspond une ou plusieurs orthographes se rapportant à un même son, par exemple le fragment "f" peut s'orthographier ph ou f. Le programme génère des mots de passe prononçables en choisissant au hasard parmi les trois types de fragment et en les concaténant en suivant les 3 règles suivantes :

* Une consonne doit être suivie d'une voyelle courte ou longue.

* Une voyelle peut être suivie d'une voyelle d'un type différent ou par une consonne.

* On ne peut pas concaténer plus de 2 voyelles à la suite les unes des autres.

Lorsqu'un fragment est choisi, le programme sélectionne au hasard une orthographe correspondant au fragment.

Notons qu'un mot de passe généré par ce programme n'intègre ni caractères numériques, ni caractères spéciaux.

---

(1) [(B. Allberty v05i059 : pwgen-random but pronounceable password generator, USENET posting in comp.sources.misc, Message-ID : 13184ncoast.UUCP, 26 November 1988) cité par D. Jobush et A. Oldehoeft dans "A survey of password mechanisms : weaknesses and potential improvements. Part 2" Computer & Security, 8 (1989) 675-689]

ANNEXE 4 : DICTIONNAIRE DES MOTS DE PASSE

Le vers Ethernet de novembre 1988 comportait un fichier dictionnaire de mots de passe qui lui permettait de continuer à se propager. Ce dictionnaire comportait 432 mots, principalement des noms et acronymes communs dont :

> aaa, academia, airplane, alphabet, animals, answer, anything, bananas, bandit, beauty, change, cat, computer, cookie, digital, discovery, dog, egghead, engine, extension, fairway, foolproof, football, format, friend, fun, hacker, hello, help, include, irishman, kernel, knight, magic, master, minimum, oracle, outlaw, password, pizza, puppet, rainbow, random, rosebud, scheme, secret, sharks, shuttle, signature, smile, spring, subway, success, summer, surfer, symmetry, tape, target, telephone, tiger, trombone, unicorn, water, wizard, zap,

et des noms de personnes et de lieu dont :

> albert, alexander, arthur, aztecs, bacchus, batman, beethoven, benz, beowolf, berkeley, beverly, bob, brenda, caroline, celtics, chester, cornelius, disney, edinburgh, edwin, einstein, garfield, gorge, graham, hamlet, japan, jessica, johnny, joshua, judith, julia, kathleen, kermit, lazarus, lee, lewis, lisa, macintosh, mack, malcolm, marvin, merlin, mozart, napoleon, newton, orwell, oxford, pacific, ronald, simon, socrates, stuttgart, toyota, yellowstone, yosemite.

(liste : Computer & Security juin 1989 p. 289)

ANNEXE 5 : RECOMMANDATIONS DE LA CNIL

La Commission Nationale de l'Informatique et des Libertés estime que l'utilisation dans le domaine médical de réseaux de transmission publics et de terminaux de type grand public (type Minitel) comporte un risque important de divulgation et d'altération d'informations nominatives de nature à porter atteinte à la vie privée et à l'intimité des personnes concernées.

En conséquence, la Commission considère que, conformément à l'article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, des mesures particulières de sécurité doivent être prises afin de garantir la confidentialité des données médicales.

A cet effet, la Commission recommande actuellement, compte tenu de l'évolution des solutions techniques proposées sur le marché, un certain nombre de mesures qui, bien entendu, doivent être adaptées ou complétées, le cas échéant, selon la finalité de l'application, la nature des informations, la configuration informatique retenue.

1. Mesures de sécurité générales

- Implantation du serveur dans un local professionnel réservé à l'usage médical, sous la responsabilité d'un médecin garant de la sécurité physique et logique des données médicales, notamment de la gestion des habilitations et droits d'accès.

- Numéro de téléphone d'appel ou code d'accès au serveur ne figurant pas dans un annuaire public.

- Procédure de contrôle d'accès de type **un code utilisateur et un mot de passe**, l'un et l'autre propres à chaque membre du personnel médical habilité à accéder au service, chacun étant d'une longueur minimale imposée de six caractères alphanumériques (si possible). Le mot de passe devrait être généré automatiquement par le système ou au moins attribué pour la moitié automatiquement par le système, l'autre moitié modifiable par l'utilisateur, devant si possible être changée régulièrement (par exemple, tous les six mois).

- Numéro d'appel du serveur et **codes utilisateur et mot de passe** communiqués aux utilisateurs par le responsable du serveur, sous pli cacheté ou en main propre, accompagné d'une notice leur rappelant le caractère confidentiel de ces codes et les sensibilisant aux problèmes de sécurité informatique et aux dispositions de la loi du 6 janvier 1978.

- Contrôle par le serveur de l'accès sélectif des utilisateurs aux dossiers de leurs patients.

- En cas de frappes incorrectes successives du mot de passe (associé à un code utilisateur correct), trois par exemple, invalidation du code utilisateur, ou tout au moins déconnexion, blocage temporaire de l'accès et message demandant à l'utilisateur d'appeler le responsable du serveur.

- Impossibilité d'être connecté à l'application à plusieurs sous les mêmes codes utilisateur et même mot de passe.

- Indication systématique à l'utilisateur de la date et de l'heure de la dernière connexion au serveur sous les mêmes codes utilisateur et mot de passe, de façon à lui permettre de détecter une éventuelle instruction dans le système et de changer, en conséquence, de mot de passe.

- Utilisation si possible, d'un numéro de dossier ou cryptage des données d'identité.

- Recours à des solutions d'identification et d'authentification des utilisateurs du type **carte à mémoire** pour les applications les plus sensibles.

2. Mesures de sécurité complémentaires :

En cas de transmission de résultats d'analyses :

- Mise en oeuvre systématique du dispositif de correction automatique des erreurs, en cas de défaut de transmission (dispositif décrit dans le guide des spécifications techniques du Minitel), ou à défaut, affichage de résultats numériques sous une forme redondante.

- Impossibilité d'éditer une liste de noms de patients.

En cas de transmission de données médicales par le réseau commuté interne de l'établissement :

- Programmation de l'autocommutateur téléphonique de l'établissement, de façon à permettre exclusivement aux postes autorisés, c'est-à-dire physiquement à certaines prises téléphoniques, l'appel du numéro réservé à la communication avec l'application.

- Impossibilité d'appeler directement le numéro interne du serveur depuis le réseau public extérieur (SDA) ou de se faire communiquer ce numéro par l'intermédiaire du standard.