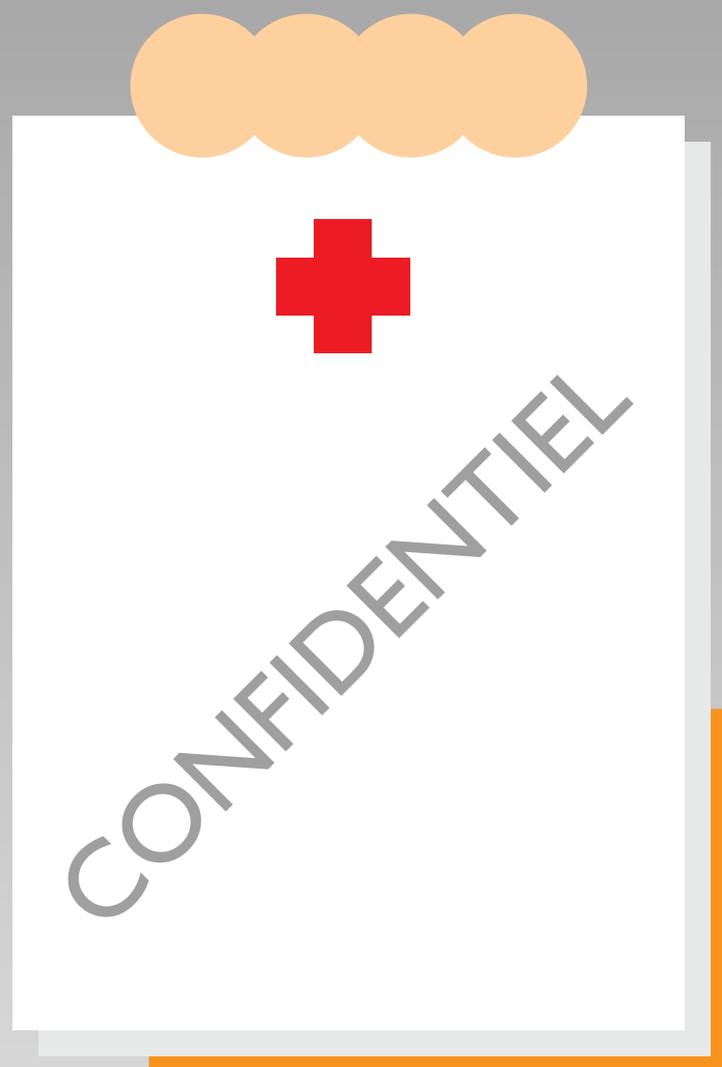
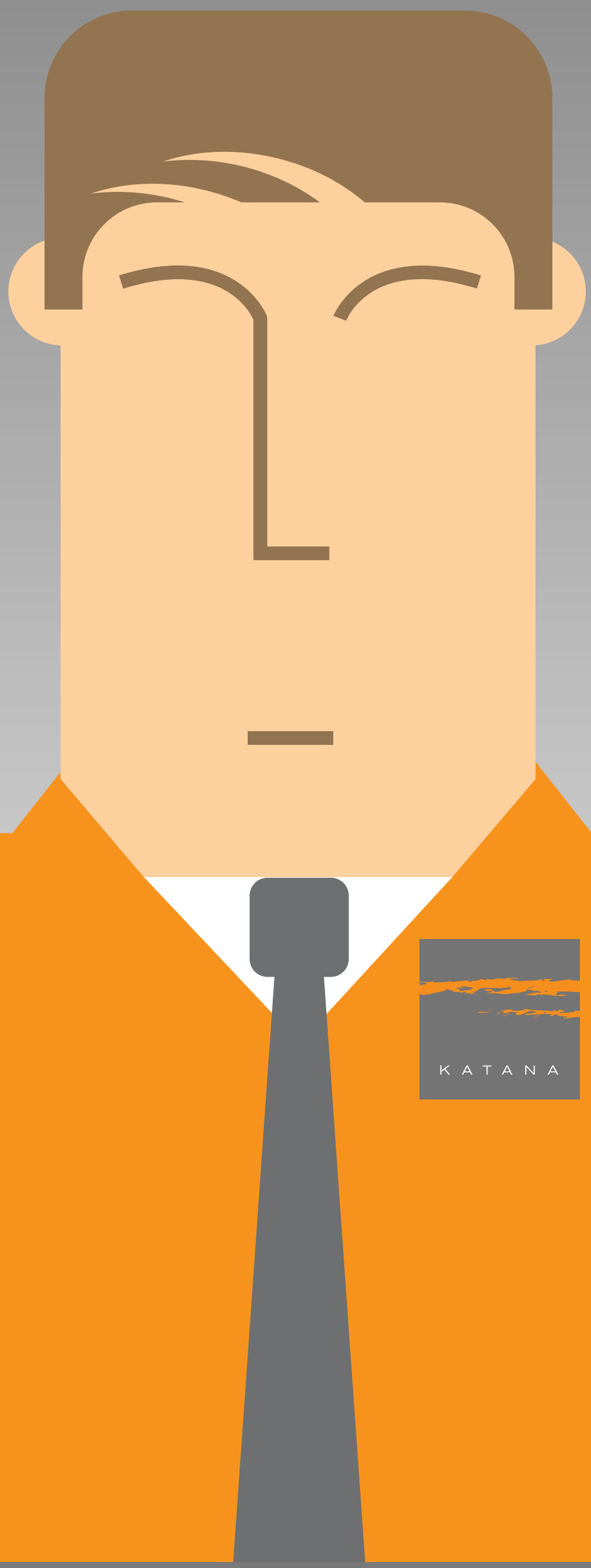
Usurpation d'identité médicale
"Un fléau méconnu qui peut coûter jusqu'à la vie"

Alors que l'usurpation d'identité économique des particuliers, peut entraîner la ruine de leur bonne cote de crédit et causer des années de problèmes et de stress, l'usurpation d'identité médicale bien moins connue peut, elle, coûter la vie.





KATANA

Résumé des bases légales sur la protection des données confidentielles.

EN GÉNÉRAL

La protection contre l'emploi abusif de données personnelles a été inscrite dans la loi fédérale sur la protection des données, du 19 juin 1992 (RS 235.1 ; LPD), en vigueur depuis le 1er juillet 1993 et dont le champ d'application couvre le traitement de données concernant des personnes physiques et morales effectué par des personnes privées ou par des organes fédéraux. L'ordonnance correspondante (RS 235.11 ; OLPD) règle différents détails d'application.

D'autres lois contiennent de nombreuses dispositions relatives à la protection de la personnalité dans des domaines particuliers. Les articles 28 et suivants du Code civil suisse, du 10 décembre 1907 (RS 210 ; CC) fixent les voies de droit applicables en cas d'atteinte à la personnalité.

DU POINT DE VUE DU DROIT PÉNAL

Les articles 34 et 35 LPD prévoient des sanctions pénales (l'amende), qui s'appliquent en cas de non-respect intentionnel des obligations de renseigner, de déclarer et de collaborer ou en cas de violation du devoir de discrétion, et ce, uniquement sur plainte.

L'article 320 alinéa 1 du Code pénal suisse (RS 311.0 ; CP) stipule que les membres d'une autorité ou les fonctionnaires qui violent leur secret de fonction sont soumis à une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

L'article 321 alinéa 1 CP prévoit que les membres de certaines professions (notamment les avocats, les notaires, les médecins, les dentistes, les pharmaciens, les sages-femmes, ainsi que leurs auxiliaires) qui auront violé leur secret professionnel seront, sur plainte, punis d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Enfin, en vertu de l'art. 321bis alinéa 1 CP, celui qui, sans droit, aura révélé un secret professionnel dont il a eu connaissance dans le cadre de son activité pour la recherche dans les domaines de la médecine ou de la santé publique, sera puni en vertu de l'article 321 CP.

DU POINT DE VUE DU DROIT CIVIL

Toute action contre une violation de la LPD qui n'est pas couverte par le champ des articles 34 et 35 LPD relève de la compétence du juge civil, conformément à l'art. 15 LPD, dans le cadre d'une procédure usuelle de droit civil régie par les articles 28, 28a et 28l CC.

Ainsi, l'article 28 alinéa 1 CC prévoit que celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe.

L'article 28a CC précise que le demandeur peut ainsi requérir du juge d'interdire une atteinte illicite, si elle est imminente, de la faire cesser, si elle dure encore, ou d'en constater le caractère illicite, si le trouble qu'elle a créé subsiste. Il peut en particulier demander qu'une rectification ou que le jugement soit communiqué à des tiers ou publié.

Enfin, sont notamment réservées les actions en dommages-intérêts et en réparation du tort moral (article 28a alinéa 3 CC).

AU NIVEAU CANTONAL

La majorité des cantons dispose de bases légales topiques régissant le domaine de la protection des droits des personnes physiques ou morales de droit privé quant aux données personnelles les concernant et qui feraient l'objet d'un traitement par l'administration cantonale en question, et les services et organisations qui en dépendent.

A Genève par exemple, la loi sur l'information, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (A 2 08 ; LIPAD), est applicable notamment aux administrations cantonale et communales, ainsi qu'aux établissements et corporations de droit public cantonaux et communaux.

L'article 37 alinéa 1 LIPAD prévoit que les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

L'article 64 alinéa 1 LIPAD traite des sanctions en cas de violation de la LIPAD et stipule que celui qui, au sein d'une institution soumise à la LIPAD, traite des données personnelles à des fins étrangères à l'accomplissement des tâches légales qui lui sont confiées est passible de l'amende, sans préjudice des peines plus fortes prévues par le droit fédéral.

KATANA

Risques liés à l'usurpation d'identité médicale

REMARQUE GÉNÉRALE

Alors que l'usurpation d'identité économique des particuliers, peut entraîner la ruine de leur bonne cote de crédit et causer des années de problèmes et de stress, l'usurpation d'identité médicale bien moins connue peut coûter la vie.

L'usurpation d'identité médicale et le mauvais usage des informations personnelles de tiers, y compris leur nom et numéros de carte d'assurance constituent une manne pour les personnes mal intentionnées et un risque pour la vie du patient dont les informations sont dérobées à son insu.

DÉFINITION

The World Privacy Forum www.worldprivacyforum.org, un organisme à but non lucratif spécialisé dans la recherche sur l'usurpation d'identités et ses risques, définit l'usurpation d'identité médicale de la façon suivante:

«Lorsqu'une personne s'approprie le nom et d'autres informations pertinentes au profil médical d'un patient, à son insu dans le but d'obtenir des soins médicaux ou des médicaments, ou lorsque cette personne utilise ces informations à des fin lucratives».

INTRODUCTION

Encore peu connus en Europe, et plus précisément en Suisse, les cas d'usurpation d'identité médicale sont un fléau aux Etats-Unis , puisque les cas d'usurpation médicale recensés sont passés de 500'000 en 2006 à 1'500'000 en 2012, soit une augmentation de plus de 200% [1].

Selon de nombreux experts, la croissance du vol d'identité médicale est en hausse en raison notamment du passage du papier à l'informatique et de son caractère hautement rentable. L'informatique contient par définition un plus grand volume de données privées et relie le réseau que composent médecins, hôpitaux et assurances. Monsieur Robert Higgins, responsable des services de sécurité chez GlassHouse (GlassHouse Technologies Inc.), précise que *« [...] sur le marché noir, les numéros de carte de crédit se négocient pour quelques dollars, alors que les numéros d'identifications médicales et ceux des mutuelles de santé se vendent pour quelques centaines de dollars».*

Le Ponemon Institute, dans une étude soutenue par Experian ProtectMyID, a publié son deuxième rapport annuel et tire les conclusions suivantes: Plus d'un million cinq-cents mille Américains ont été victimes d'usurpations d'identité médicales. Le rapport estime que le coût moyen pour résoudre chaque vol de ce type est d'environ USD 20'000.- (vingt-mille dollars US) [2]

Le World Privacy Forum précise enfin que *«le vol d'identité médicale, bien qu'il soit le crime pouvant causer le plus grand tort à ses victimes, est le moins documenté et le moins étudié. Il est aussi le plus difficile à découvrir après qu'il ait été commis».*

QUI SONT LES AUTEURS DES VOLS D'IDENTITÉS

Les voleurs d'identité médicale sont souvent des proches, des collaborateurs ou des fournisseurs ayant accès aux données. Toutefois, le côté très lucratif, le peu de sanctions ou encore la difficulté de détection commencent à susciter l'intérêt des réseaux de crime organisé. Avec l'émergence d'Internet et des réseaux sociaux, des vols avec demande de rançon peuvent aussi arriver.

En effet, comme le rapporte ZD Net, un hôpital américain a été victime d'un rançonnement de USD 10'000'000.- (dix millions de dollars US) pour des données médicales affectant plus de huit millions de patients.

Le pirate menaçait de diffuser les données sur le Web si l'hôpital ne s'acquittait pas de la somme exigée. Le FBI a confirmé qu'il s'agissait là du deuxième cas recensé [3] **cf. Article page 19**

CONCLUSION

"En conclusion, il est important de noter qu'en plus de tous les risques énumérés ci-dessus, l'établissement hospitalier médicaux eux-mêmes courent un sérieux danger des suites de vols d'identité. En effet, ces derniers peuvent être poursuivis de dommages et intérêts de la part des personnes lésées, ou encore en violation du secret professionnel et donc passibles de plaintes pénales selon le Code Pénal suisse (violation du secret professionnel – art 320).

Et ce n'est pas tout. Car si ces risques la peuvent entrainer une procédure judiciaire longue et ardue pour le management, ils résultent souvent en une perte de réputation, qui représente un dommage aussi bien financier qu'économique bien plus grave pour la pérennité de l'établissement médical et tout le personnel soignant et administratif. Il faudra parfois de très longues années et d'énormes ressources pour se remettre des conséquences d'un tel danger, qui sommes toutes aurait pu être évité dès le départ, si les précautions nécessaires à disposition avaient été appliquées. "

Sur la base de ce qui précède, il convient de souligner la nécessité pour tout établissement ayant accès à des informations médicales de mettre en place tous les moyens possibles afin de limiter le vol et les dommages qui s'en suivent. Il est donc recommandé d'avoir une attitude proactive plutôt que réactive.

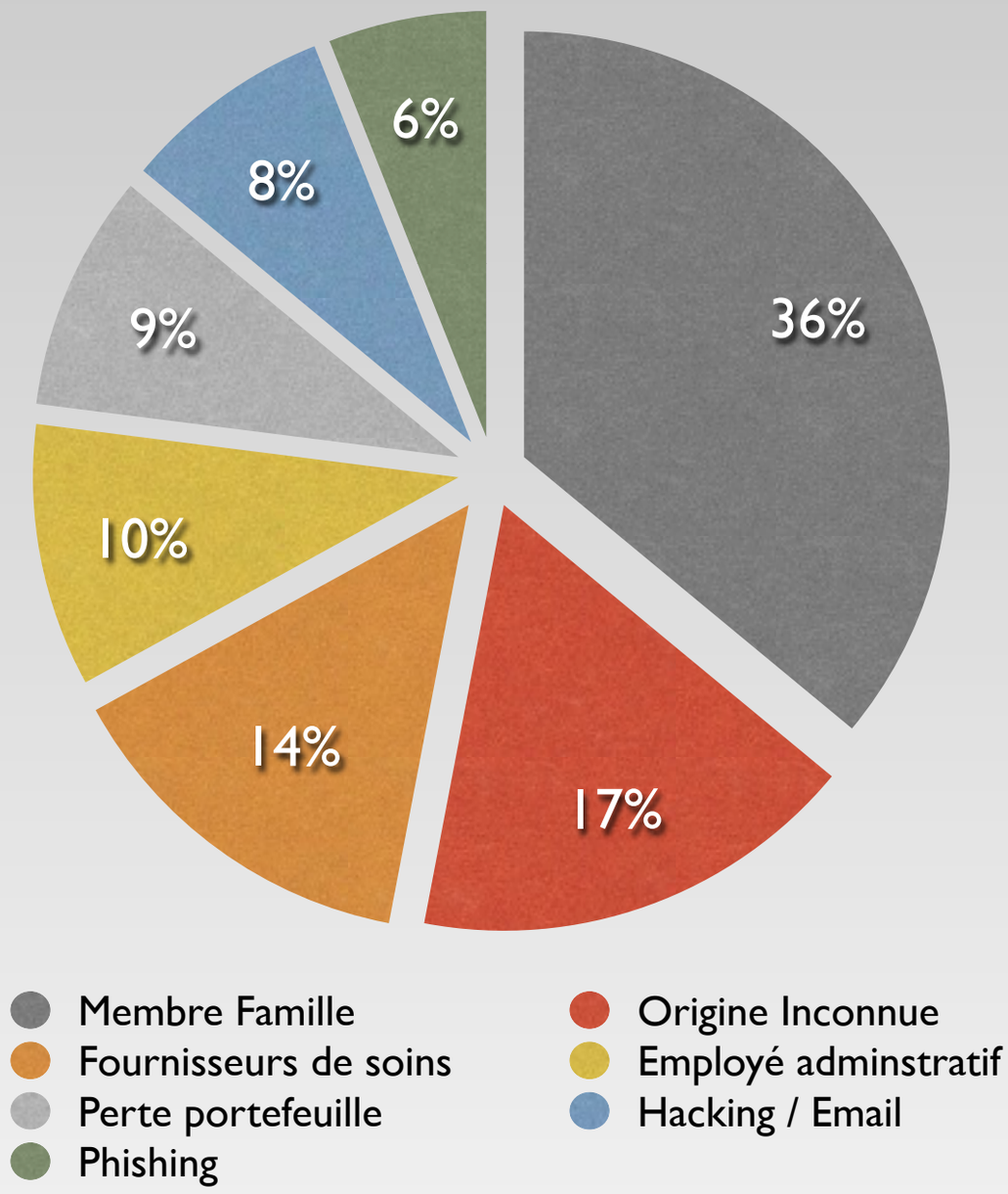
ET POUR FINIR VOICI QUELQUES CONSEILS POUR PROTÉGER VOS DOCUMENTS CONFIDENTIELS :

- Limiter l'accès aux données à certaines personnes ;
- Contrôler et limiter l'utilisation de certains appareils tels que téléphones portables, clefs USB, etc. ;
- Mettre en place des procédures strictes pour la destruction des documents confidentiels sur support papier ou informatique ;
- Maintenir une procédure de stockage sécurisé à l'aide de conteneurs fermés à clefs pour les documents confidentiels destinés à être détruits ;
- Ne pas laisser des tiers détruire les documents papiers et les supports informatiques, s'assurer que la destruction à lieu sur le site et n'encourt donc aucun risque lié au transport.

CHIFFRES CLEFS:

- •36% vol effectué par un membre de famille
- •17% origine inconnue
- •14% fournisseurs de soins mis en cause
- •10% effectué par un employé administratif malveillant travaillant pour un prestataire de santé

ORIGINE DES VOLS D'IDENTITÉ MÉDICALE:



Source: Lemondeinformatique.fr

OÙ SE TROUVENT LES INFORMATIONS POUR LE VOL D'IDENTITÉ.

Les cabinets médicaux, les hôpitaux, cliniques et entreprises d'assurance sont les établissements possédant le plus d'informations sur le profil du patient et constituent donc la cible idéale pour les usurpateurs d'identité.

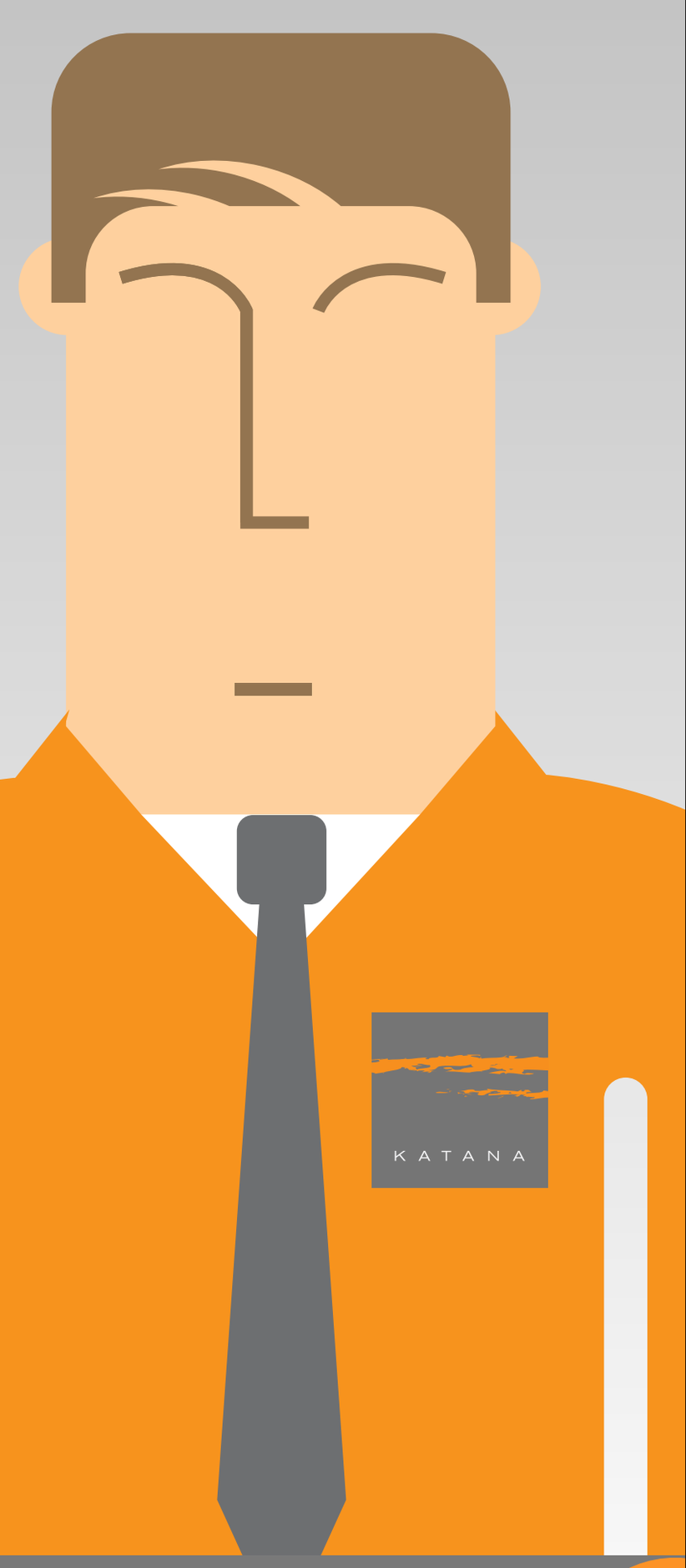
QUE PEUT FAIRE UNE PERSONNE MAL INTENTIONNÉE EN USURPANT VOTRE IDENTITÉ MÉDICALE?

L'usurpateur d'information médicale peut utiliser des informations de tiers pour obtenir des soins médicaux, des produits et médicaments nécessitant une ordonnance ou encore faire des réclamations médicales frauduleuses.

Certains usurpateurs d'informations médicales sont motivés uniquement par l'aspect lucratif du vol de données personnelles.

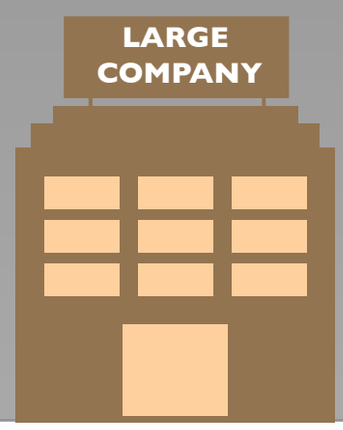
"Les données individuelles que le personnel d'un cabinet médical est amené à traiter appartiennent à la catégorie des données devant faire l'objet d'une protection toute particulière, car l'état de santé d'un patient est confidentiel par excellence."

Source: Préposé fédéral à la protection des données et à la transparence (PFPDT)



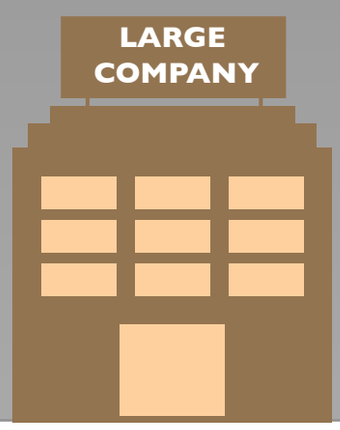
1. *Source The World Privacy Forum First report 2006 and internet web site*
2. *SourcePonemon Institute, article lemondeinformatique.fr*
3. *Source ZD Net article*

Conseils pour la sécurité



Simplifier la destruction de documents confidentiels au moyen d'une politique de "totale destruction", afin de s'assurer que tous les documents sont stockés dans des conteneurs sécurisés et ensuite détruits d'une manière sure.	Les petites entreprises partagent souvent leur espace avec d'autres organisations et partagent parfois également les photocopieuses, imprimantes et espaces de stockage. De ce fait, il est absolument essentiel que tous documents confidentiels soient stockés dans des conteneurs sécurisés et ensuite détruits de la manière la plus sur et dans des délais très courts afin d'éviter tous risques de tomber dans de mauvaises mains.	Les grandes entreprises ont de nombreux employés, dont tous ne devraient avoir accès aux renseignements confidentiels. En appliquant une politique de « totale destruction » les entreprises éliminent le processus de décision quant à quels sont les documents confidentiels et les quels ne le sont pas, et s'assurent ainsi que tous les documents sont immédiatement détruits.
Assurez-vous que tout dispositif de sauvegarde électronique (tels disques durs, clé USB et mémoire de photocopieuses) sont broyés sur place avant de vous en débarrasser. Ceci est la seul manière d'éliminer tous les risques.	En actualisant (modernisant) leur système informatique, les petites entreprises ont souvent tendance à utiliser des logiciels de destruction qui effacent le disque dur. Cependant, ceci peut entrainer des couts importants par la suite – la destruction physique des disques durs est la seule et unique manière 100% sure de détruire les données électroniques et éviter que l'information ne tombe dans les mains de malfaiteurs.	Les grandes entreprises emploient souvent des consultants informatique pour effacer les données électroniques sauvegardées en encourant le risque d'exposer l'information confidentielle a un personnel non autorisée. Assurez-vous que votre information confidentielle le reste en engageant une société qui se spécialise dans la destruction de dispositifs électroniques et qui le fait sur place. (disques durs, clés USB et mémoire de photocopieuses).
Protégez vos documents électroniques en limitant l'accès aux dossiers confidentiels et en cryptant l'information confidentielle sur les dispositifs portables.	Lorsque les employés de petites entreprises utilisent des ordinateurs portables ou travaillent de la maison, il est plus difficile de préserver l'information confidentielle. Il est essentiel d'assurer la sécurité et la confidentialité de tous documents en cryptant l'information sur les dispositifs personnels et bien sûr de limiter l'accès « off site » au personnel autorise uniquement.	Nombreuses sont les larges entreprises qui donnent à leurs employés des dispositifs portables afin qu'ils soient accessibles à tous moments. Cependant si les dispositifs non cryptes sont voles ou perdus ils peuvent mettre en danger toute la sécurité de la société.

Conseils pour la sécurité



Développez et renforcez les procédures de sécurité pour assurer que les employés apprennent à manipuler l'information confidentielle en conformité avec les lois et règlementations locales.	Avec peu d'employés, de nombreuses petites entreprises n'établissent pas de procédures de sécurité obligatoires pour leurs employés. Ceci cause des problèmes en cas de doute et engendre des erreurs graves dans la manipulation de documents confidentiels.	Dans les grandes entreprises il est plus difficile de contrôler régulièrement la sécurité au travers de l'entreprise toute entière. Le meilleur moyen de s'assurer que les employés suivent les procédures mises en place est de nommer des employés exclusivement responsables de gérer les questions de sécurité de l'information, d'établir des règles strictes et claires à cet effet et de former le personnel régulièrement.
Menez des audits afin de déterminer les risques et besoins de votre société	Peu de petites entreprises ont un employé responsable de la sécurité de l'information. Choisissez un employé qui sera chargé de mener des vérifications périodiques afin d'identifier les risques de sécurité qui peuvent apparaitre a tous moment.	Avec un grand nombre d'employés il est parfois difficile pour une société de suivre efficacement les opérations quotidiennes. Sachant cela, il est essentiel que les entreprises effectuent un audit de sécurité global afin de s'assurer qu'il n'y ait aucune faille dans sa sécurité et que les procédures sont bien appliquées.
Prenez connaissance des conditions de sécurité requises par la loi, et assurez- vous que votre entreprise est en règle.	Les petites entreprises ignorent souvent leurs obligations légales de sécurité requises, et s'ils ne s'en acquittent pas pourraient se retrouver passible d'une grosse amande qui pourrait même mettre leur affaire en difficulté financière	Il est très important pour les larges entreprises d'être en règle avec les lois en matière de sécurité en constante évolution. Même si votre société était en règle par le passe, des changements réglementaires locaux peuvent entrainer votre entreprise à devoir payer de fortes amandes qui pourraient affecter votre performance.

Comparatif de risque du système Katana vs système hors site.

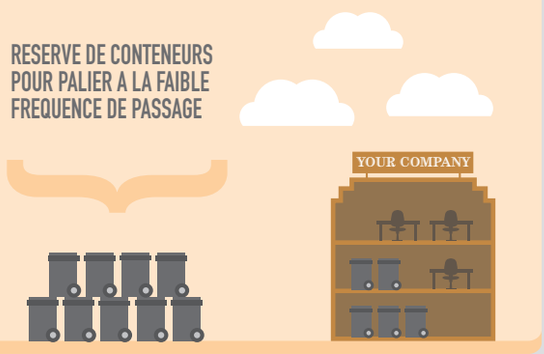
OFFSITE VS ONSITE

SHREDDING

DESTRUCTION HORS SITE

1 STOCK DE CONTENEURS

RESERVE DE CONTENEURS POUR PALIER A LA FAIBLE FREQUENCE DE PASSAGE



2 RELEVE DES CONTENEURS

ETAPE DE RELEVE REPETEE JUSQU'A **22 X / JOUR**

3 TRANSPORT DOCUMENTS

4 DESTRUCTION OFFSITE

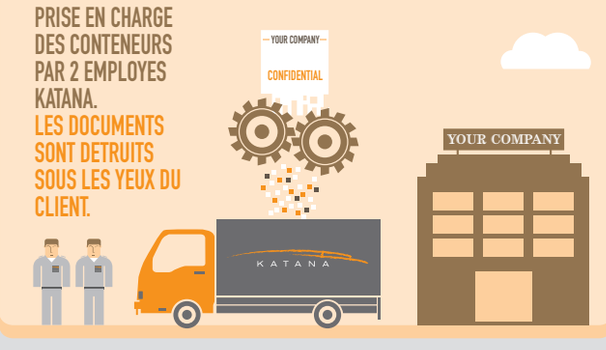
24 HEURES OU PLUS AVANT QUE VOS DOCUMENTS NE SOIENT DETRUITS

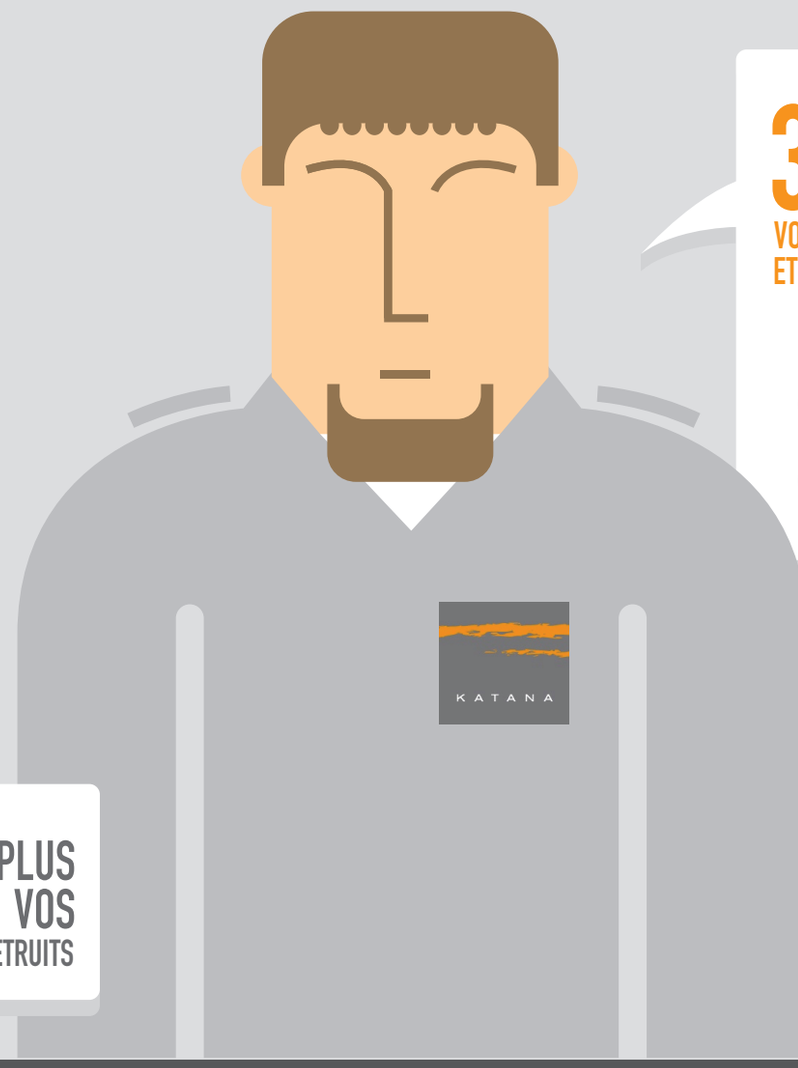
DESTRUCTION SUR SITE

1 MISE EN PLACE

2 DESTRUCTION SUR SITE

PRISE EN CHARGE DES CONTENEURS PAR 2 EMPLOYES KATANA.
LES DOCUMENTS SONT DETRUITS SOUS LES YEUX DU CLIENT.





30 MINUTES APRES NOTRE PASSAGE
VOS DOCUMENTS SONT DETRUITS ET TOUS LES RISQUES ELIMINES

(NORME DIN 32757-1-3)

Frais supplémentaires: Transport, location, manutention	Occupation d'espace inutile	Hacktivisme, terrorisme économique	Incendie camion	Detournement, vol du camion	Vol de conteneurs / documents	Distance de parking élevée (risques d'attaque, vol du camion / conteneurs)	Trajets suivis par GPS, risque de hacking / vol

KATANA