1 Préambule

La présente Charte informatique définit les conditions générales d'utilisation du Système d'Information au sein du Centre de Recherche et du Siège de l'Institut Curie. Elle a pour objectif d'informer les Utilisateurs des exigences de sécurité. Le bon fonctionnement du Système d'Information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la protection des données.

1.1 Définitions

- **Etablissement** désigne ici le Centre de Recherche de l'Institut Curie, son Siège, ou les deux.
- **Utilisateur interne** : toute personne physique travaillant sur les sites de l'Institut Curie et disposant à ce titre d'un identifiant dans l'annuaire informatique de l'Etablissement.
- **Utilisateur externe** : toute personne physique ne disposant pas d'un identifiant dans l'annuaire informatique de l'Etablissement, et accédant au Système d'Information de l'Etablissement ou à Internet dans le cadre d'un usage professionnel en lien avec l'activité de l'Institut Curie.
- **Le Système d'Information** est l'ensemble organisé de ressources technologiques (matérielles, logicielles, applications, bases de données et réseaux de télécommunication locaux) et d'une structure organisationnelle et humaine, qui permettent de collecter, stocker, traiter et diffuser de l'information.
- **Terminal :** tout dispositif électronique, fourni par l'employeur ou appartenant à l'Utilisateur, utilisé pour l'accès au Système d'Information professionnel ou personnel autorisé : un ordinateur fixe, un ordinateur portable, une tablette, un smartphone, un téléphone fixe, un fax etc.
- **BYOD :** Bring Your Own Device désigne l'usage de tout Terminal personnel à des fins professionnelles

1.2 Champ d'application

La présente Charte s'applique à l'Etablissement ainsi qu'à tout Utilisateur interne ou externe du Système d'Information.

2 Conditions d'utilisation du Système d'Information

L'Etablissement rappelle que les outils mis à la disposition de l'Utilisateur tels que la téléphonie, la visioconférence, l'impression/photocopie/fax, Internet, la messagerie et les outils de travail collaboratif, sont destinés à un usage professionnel.

Sous certaines conditions, l'Utilisateur peut se connecter au réseau de l'Etablissement avec son propre Terminal que ce soit par voie filaire, par le WiFi d'entreprise, ou par accès distant (de type VPN). Il devra se signaler à la DSI[1] avant toute tentative de connexion. La DSI lui fournira toutes les informations de configuration nécessaires. L'Etablissement n'offre cependant pas de garantie de compatibilité avec l'ensemble des Terminaux apportés par l'Utilisateur.

2.1 Droits d'accès au Système d'Information

Les droits d'accès au Système d'Information sont basés sur le compte utilisateur.

Le compte utilisateur est défini par un identifiant unique et un mot de passe ; il donne à l'Utilisateur des droits d'accès à des ressources informatiques de l'Etablissement, définis en fonction du poste et du profil de l'Utilisateur.

Ce compte, associé à une et une seule personne physique, est strictement personnel et confidentiel et non cessible. L'Utilisateur s'engage à ne pas le divulguer, ni le céder à des tiers.

L'Utilisateur est seul responsable de l'utilisation de son compte, ainsi que de tout préjudice direct ou indirect causé à lui-même ou à des tiers du fait de l'utilisation des systèmes informatiques. Il s'engage

- à bien protéger son mot de passe comme décrit dans la note en Annexe. L'utilisateur ne doit pas utiliser le même mot de passe pour ses applications professionnelles et ses applications privées.

[1] *DSI : Direction des Systèmes d'Information*

- à ne pas falsifier ou masquer intentionnellement sa véritable identité. Toute utilisation du Système d'Information effectuée au moyen de son compte sera réputée avoir été faite par l'Utilisateur, sauf preuve du contraire apportée.

Il est strictement interdit

- de mettre en place tout moyen de contournement des contrôles d'accès au Système d'Information.
- d'accorder l'accès au Système d'Information à toute personne qui n'a pas été dument répertoriée ni par la DRH[2] ni par la DSI.

2.2 Utilisation résiduelle privée

L'utilisation résiduelle à titre privé de ces outils ou des réseaux sociaux peut être tolérée dans la limite où :

- elle est non lucrative et raisonnable, tant dans sa fréquence que dans sa durée.
- elle ne nuit pas à la qualité du travail de l'Utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.
- elle ne nuit pas à l'image ou à la réputation de l'Etablissement (participation à des forums, blogs et groupes de discussion véhiculant des messages à caractère terroriste, pédophile, haineux, raciste, injurieux ou portant atteinte à l'ordre public ou aux bonnes mœurs etc.)
- elle respecte la règlementation en vigueur

2.3 Gestion des absences prolongées et des départs

En cas de départ, ou d'absence prolongée, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. En tout état de cause les données non situées dans un espace identifié comme privé[3], sont considérées comme appartenant à l'Établissement qui pourra en disposer librement.

Le départ d'un Utilisateur entraîne la désactivation de son compte informatique selon les modalités décrites dans la note en Annexe.

L'Utilisateur est responsable de son espace privé, il lui appartient lors de son départ définitif de récupérer le contenu de cet espace, et de libérer la place occupée sur le Système d'Information. La responsabilité de l'Etablissement ne peut être engagée quant à la conservation des données figurant dans cet espace.

3 Les outils de communications

3.1 La messagerie électronique

Adresse électronique

L'Etablissement met à disposition de l'Utilisateur une adresse électronique nominative associée à une boite à lettres lui permettant d'émettre et de recevoir des messages électroniques.

L'utilisation de cette adresse nominative est de la responsabilité de l'Utilisateur. Ainsi l'Utilisateur s'engage à :

- Utiliser cette adresse électronique à des fins strictement professionnelles en dehors des cas prévus à l'article 2.2 de la présente Charte.
- faire preuve de vigilance vis-à-vis des messages reçus notamment les courriers non sollicités (« spams ») pouvant contenir des informations falsifiées ou frauduleuses, des virus ou des liens vers des sites malveillants. En effet, les messages et leurs pièces jointes jouent souvent un rôle central dans les cyberattaques.

[2] *DRH : Direction des Ressources Humaines*
[3] *Par exemple un dossier ou un fichier comportant dans le nom "privé_nom_prénom, ou nommé « perso » ou « personnel »*

- ne pas utiliser à des fins professionnelles les boites email autres que celles mise à disposition par l'Etablissement ou ses Tutelles (INSERM, CNRS, …), à plus forte raison celles « gratuites » (type Gmail, Live ou Yahoo) qui exploitent les données transmises. L'usage de messageries tierces est notamment prohibé pour échanger des données sensibles[4].
- Et en tout état de cause, faire preuve de la correction normalement attendue dans tout type d'échange à l'égard de ses interlocuteurs

Messages électroniques

Tout message reçu ou émis avec l'adresse professionnelle est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[5] ou s'il est stocké dans un espace privé de données

A défaut d'une telle identification, et lorsqu'ils sont nécessaires à la poursuite de l'activité de l'Etablissement, l'employeur peut à tout moment accéder librement aux messages.

Toutefois, l'Utilisateur ne doit pas transformer tous ses messages de nature professionnelle en correspondance privée. En cas de risque d'atteinte à la sécurité, de continuité de service, ou d'un risque de voir sa responsabilité engagée, l'Etablissement peut accéder aux fichiers ou contenu de la boite de messagerie identifiés comme « privé » en présence de l'Utilisateur ou en cas d'absence s'il a été dument informé.

Contenu des messages

Il est strictement interdit d'échanger des messages comportant les contenus :

- à caractère illicite quelle qu'en soit la nature. En particulier il est interdit de diffuser de contenus portant atteinte à la vie privée d'autrui (atteinte à la tranquillité par des menaces, atteinte à l'honneur par la diffamation ou par l'injure)
- portant atteinte à l'image et à la réputation de l'Institut Curie et/ou de ses Etablissements.
- portant atteinte à l'intégrité du Système d'Information de l'Institut Curie et/ou de ses Etablissements

3.1.1 Statut et valeur juridique des messages

Il est rappelé que les messages électroniques engagent l'Institut Curie. L'Utilisateur doit, par conséquent, être vigilant concernant la nature des messages qu'il échange.

3.1.2 Contrôle et Analyse de la messagerie

Pour préserver le bon fonctionnement du réseau et des services, des dispositifs de contrôle de la messagerie sont mis en place ; des quotas peuvent être appliqués sur la taille des messages reçus et envoyés, sur le nombre de messages envoyés par période de temps, ou sur la capacité totale de la boîte de la messagerie.

3.2 Internet

Internet est un outil de travail ouvert à des usages professionnels même si une utilisation résiduelle privée précisée plus haut, peut être tolérée.

Lorsque l'Utilisateur utilise Internet, il laisse sur des serveurs externes, des traces de connexion notamment celles concernant l'Etablissement. L'Utilisateur s'engage donc à rester vigilant lorsqu'il utilise Internet afin de ne pas porter de préjudice à l'Institut Curie et/ou ses Etablissements.

---

[4] *Au sens de la CNIL, ce sont des données à caractère personnel qui font apparaître, directement ou indirectement : les origines raciales ou ethniques, les opinions politiques, philosophiques syndicales ou religieuses, la vie sexuelle, les infractions, les condamnations ou mesures de sûreté, le numéro de sécurité sociale, des appréciations sur les difficultés sociales des personnes, des données biométriques, des données génétiques, des données relatives à la santé*

[5] *Par exemple, les messages comportant les termes "privé" dans l'objet ou le sujet des messages*

Contrôle et Analyse de l'Internet

L'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Etablissement et qui permettent d'assurer :

- un filtrage des sites web : sont bloqués les sites illégaux (apologie du terrorisme, vente d'armes et de drogues…) ou des sites sans rapport avec l'activité professionnelle (pornographie, jeux en ligne).
- la traçabilité des accès Internet : les données de connexion sont enregistrées dans des fichiers de traces et sont conservées sur une période de six mois au moins, conformément à la déclaration CNIL qui a été faite. Les administrateurs peuvent analyser ces traces dans le cadre d'une maintenance ou de la recherche des causes d'un dysfonctionnement technique tout en respectant leur devoir de discrétion et de confidentialité.

3.3 La téléphonie

L'Etablissement rappelle que l'utilisation de la téléphonie est destinée à un usage professionnel et que seul un usage résiduel à titre privé peut être toléré.

Des relevés pourront être établis, et en cas d'usage manifestement abusif de la téléphonie à des fins privées, l'Utilisateur en sera informé et des sanctions pourront être prises si nécessaire dans le respect des règles légales en vigueur.

3.4 Les réseaux sociaux

Les réseaux sociaux sont des mines d'information pour les experts de la collecte de données et des pirates.

Il est interdit de communiquer sur un réseau social sur et au nom de l'Etablissement aussi bien dans la sphère privée que professionnelle, sauf autorisation expresse de l'employeur.

Une publication sur un réseau social est soumise aux mêmes règles que si elle est diffusée par la messagerie électronique ou sur un blog ou sur une page personnelle ou sur tout autre moyen mis à la disposition de l'Utilisateur par l'Etablissement.

3.5 Les services en ligne

Afin d'assurer la continuité de service, l'Utilisateur doit privilégier le dépôt de ses fichiers professionnels dans les serveurs de l'Etablissement qui mettent à disposition des espaces de travail sécurisés partagés par les membres de son équipe.

Les logiciels de stockage et de partage de fichiers externalisés en Cloud offrent un moyen pratique d'accéder à des données en toute circonstance. Leur usage dans un contexte professionnel doit toutefois se faire en respectant certaines précautions en matière de sécurité et de confidentialité conformément à la note en Annexe. En particulier, leur usage est prohibé lorsqu'il s'agit des données de santé ou des données à caractère personnel.

3.6 Accès Distant

Le service d'accès distant permet à l'Utilisateur d'accéder à distance et de manière sécurisée au Système d'Information de l'Etablissement.

Selon la sensibilité des ressources informatiques auxquelles l'Utilisateur souhaite accéder, plusieurs solutions d'authentification peuvent être requises : le compte utilisateur comprenant un identifiant et un mot de passe et/ou un code supplémentaire à valider.

Le service d'accès distant est soumis aux mêmes conditions d'utilisation du Système d'Information que celles appliquées au sein de l'Etablissement, notamment celles qui portent sur la confidentialité et l'incessibilité du compte utilisateur ainsi que ses droits d'accès.

4 Protection des données

L'usage des Terminaux personnels à des fins professionnelles est de plus en plus répandu (BYOD) notamment pour accéder aux messages électroniques ou à des documents stockés sur les serveurs de l'Etablissement. Or ces Terminaux présentent un risque élevé de perte ou de vol et les données contenues, professionnelles ou privées, sont rarement protégées par un chiffrement[6].

Ainsi pour limiter les risques de fuite de données, les Terminaux et les périphériques de stockage (clé USB, disque dur externe etc.), qu'ils soient professionnels ou personnels, doivent être protégés par chiffrement dès lors qu'ils contiennent des données professionnelles.

Attention, le chiffrement ne protège pas contre la perte des données mais uniquement contre leur divulgation. Il faut donc réaliser une copie des données en effectuant une sauvegarde régulière sur les serveurs de l'Etablissement.

5 Devoir de signalement

L'Utilisateur a l'obligation de signaler à son responsable, ou au RSSI[7], ou, à défaut, à la DSI, dans les meilleurs délais :

- la perte ou le vol de son mot de passe, ou l'usurpation de son identité
- la perte ou le vol matériel contenant des données professionnelles, que ce matériel soit personnel ou fourni par l'employeur
- tout dysfonctionnement constaté ou toute anomalie découverte telle un virus ou une intrusion dans le Système d'Information.

D'une façon générale toute suspicion d'atteinte à la sécurité du Système d'Information ou tout manquement substantiel à cette Charte doit être signalé.

L'Etablissement pourra prendre toute mesure pour protéger ses intérêts et la confidentialité des données contenues sur le matériel perdu ou volé, notamment en choisissant de supprimer la totalité des données, dans la mesure du possible.

6 Propriété intellectuelle

L'utilisation des ressources informatiques implique le respect des droits de propriété intellectuelle de l'Institut Curie ainsi que ceux de ses partenaires et plus généralement de tout tiers titulaire de ces droits.

L'Utilisateur s'engage donc à

- utiliser les logiciels dans les conditions des licences souscrites
- ne pas reproduire, copier, diffuser, modifier ou utiliser les fichiers (textes, sons, images, logiciels ou autres créations protégées par le droit d'auteur) sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

L'Etablissement se réserve le droit de bloquer tout téléchargement de fichiers contenant de manière manifestement indue des données soumises à copyright / droits d'auteur.

7 Respect de la loi Informatique et Libertés

L'Utilisateur a l'obligation de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel conformément à la législation dite « Informatique et Libertés ».

[6] *Chiffrement : Le chiffrement est une méthode permettant de renforcer la sécurité d'un message ou d'un fichier en brouillant son contenu de sorte que seules les personnes disposant de la clé de chiffrement appropriée pour les déchiffrer peuvent les lire*

[7] *Responsable de la Sécurité des Systèmes d'Information*

Les données à caractère personnel désignent toute information qui permet d'identifier une personne physique, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui la caractérisent.

Tout Utilisateur, amené dans l'accomplissement de son travail, à constituer des fichiers soumis aux dispositions de la loi informatique et libertés, c'est-à-dire contenant des données à caractère personnel, est responsable de s'assurer de l'accomplissement des formalités requises par la CNIL conformément aux procédures internes à l'Etablissement. Il doit veiller à mettre en place et conserver un traitement de données conformes aux dispositions légales, et à en informer le RSSI ou, à défaut, la DSI.

Il est rappelé que la transmission à un tiers d'un fichier contenant des données à caractère personnel non déclaré à la CNIL est illicite.

8 Contrôle et Analyse

L'Etablissement est dans l'obligation légale de mettre en place un système de journalisation[8] des accès Internet, de la messagerie, de la téléphonie, de l'ensemble des applications et des données échangées au travers de Système d'Information.

Des dispositifs de traçabilité sont mis en place conformément aux déclarations faites auprès de la CNIL[9].

Il est rappelé que les administrateurs qui bénéficient d'accès étendus sont, par ailleurs, soumis à une obligation de confidentialité accrue.

Dans le cadre d'une procédure judiciaire ces fichiers seront mis à la disposition de la justice « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ».

En vertu de la loi « informatique et libertés » l'Utilisateur dispose d'un droit d'accès et de rectification aux données qui le concernent. Les droits d'accès au Système d'Information impliquent l'acceptation par tout Utilisateur de ses dispositifs de journalisation.

9 Sanctions applicables

L'Etablissement se réserve le droit de prendre des sanctions à l'encontre de tout Utilisateur qui ne respecte pas les dispositions de la présente Charte, notamment dans les cas suivants :

- l'Utilisateur fait un usage des services informatiques de nature à porter préjudice à l'Institut Curie ou aux tiers.
- l'Utilisateur effectue des actes de piratage par exemple en diffusant ou en reproduisant des données protégées par la propriété intellectuelle.
- l'Utilisateur fait un usage abusif des ressources informatiques à des fins extra-professionnelles.
- l'Utilisateur ne respecte pas les lois ou règlement en vigueur

Les sanctions peuvent aller d'un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, des droits d'accès au Système d'Information, à un licenciement. Des poursuites judiciaires, civiles ou pénales pourront être mises en œuvre le cas échéant.

10 Entrée en vigueur de la charte

La présente Charte prend effet en date du (à compléter). Elle annule et remplace tous les autres documents ou charte relatifs à l'utilisation du Système d'Information de l'Etablissement.

Elle est annexée au règlement intérieur.

---

[8] *Conservation des informations techniques de connexions telles que l'heure d'accès, l'adresse IP de l'Utilisateur du Terminal et du serveur accédé, et informations spécifiques telles que l'adresse d'un site Web (« URL ») ou le destinataire d'un message électronique*

[9] *CNIL Commission Nationale de l'Informatique et des Libertés*

11 Annexes

11.1 Filtrage URL/ La protection des mots de passe

11.2 Du bon usage du cloud et des services en ligne

11.3 Gestion des coûts de téléphonie

11.4 Gestion des départs

Institut Curie – Centre de Recherche Septembre 2013

Note concernant la protection des mots de passe

Régulièrement, des utilisateurs du Centre de Recherche et des Services Institutionnels sont victimes d'un vol d'identifiant et de mot de passe et deviennent ensuite à leur insu des spammeurs. Dès qu'il a connaissance d'une telle situation, le Service Informatique bloque systématiquement le compte piraté et prend contact avec la victime.

En premier lieu, nous vous rappelons qu'il est indispensable que chacun garde **secret** son mot de passe professionnel. Même si vous pensez que vos données n'ont rien de confidentiel, votre compte une fois usurpé devient en effet lui-même une faille dans le système d'information de l'Institut Curie.

La cause la plus fréquente d'usurpation d'identité est le Phishing (« Hammeçonnage ») : la victime répond à un mail ou remplit un formulaire sur internet dans lequel elle divulgue son identifiant et son mot de passe. Cette année l'Institut en a recensé au moins six.

En dehors de l'Institut Curie, le wifi public présente aussi des risques importants de sécurité : disponible dans les lieux publics (cafés, aéroports, hôtels...), très pratique et ouvert à tous, il ne nécessite généralement aucune clé de protection (WEP ou WPA) et **les données y circulent donc en clair**.

Dès lors, toute personne malveillante évoluant dans cette zone de couverture wifi peut facilement capter les identifiants et les mots de passe que vous saisissez pour entrer dans vos espaces personnels dont la page d'authentification n'est pas sécurisée (Protocole HTTP simple au lieu du HTTP**S** sécurisé). Pour peu que vous ayez utilisé votre mot de passe Curie pour vous connecter à ce type de site, votre compte Curie est susceptible d'être piraté très rapidement ensuite.

Concernant les réseaux sociaux, ou de commerce en ligne, la plupart assurent une connexion sécurisée mais il suffit que l'un d'eux subisse un vol de données comme cela arrive fréquemment (LinkedIn en juin 2012) pour que vos données de connexion soient potentiellement exposées sur Internet ou exploitées directement par un malfaiteur.

Aussi, dans le but de bien protéger votre mot de passe professionnel, il vous est demandé :

- **de ne pas utiliser le wifi public non-sécurisé pour un usage professionnel ;**
- **de proscrire impérativement l'utilisation du mot de passe professionnel pour toute application personnelle.**

Réciproquement et plus généralement, pour une meilleure protection de vos données, nous vous recommandons vivement d'utiliser des mots de passe différents selon les sphères d'utilisation (professionnelles, personnelles, bancaires, e-commerce, etc.).

Nous vous remercions pour votre compréhension et collaboration,

You-Heng EA
Service Informatique

Du bon usage du Cloud et des services en ligne

Ce document présente un ensemble de recommandations pour la protection des données traitées dans le Cloud.

1. Définitions

1.1 Le Cloud

Le « Cloud Computing » ou « l'Informatique dans le nuage » est un ensemble de services, gratuits ou payants, de stockage d'information, d'échanges d'information ou de calcul, hébergés sur des serveurs distants appartenant à des sociétés spécialisées, et accessibles via Internet.

Les datacenters, les serveurs et les réseaux qui supportent les services en ligne sont rarement connus de leurs usagers (d'où le terme de « nuage ») sauf s'ils sont décrits dans le cadre d'un contrat bipartite d'hébergement externalisé.

Dans un modèle dit « gratuit », les hébergeurs se rémunèrent principalement sur l'exploitation commerciale des données déposées par les usagers et sur la publicité ou le marketing qu'ils peuvent faire ou vendre autour de ces informations. Dans les modèles payants, sont vendus de l'espace de stockage, de la puissance de calcul, une sécurité renforcée, etc.

Ces solutions sont-elles utilisables dans le domaine du soin et de la recherche ? Qui est concerné ?

Le Cloud a été initialement destiné au grand public pour des usages personnels, notamment les offres de messagerie électronique (Gmail, Yahoo, …) ou des services de stockage en ligne (Dropbox, Google Drive, …).

Lorsqu'il est utilisé à des fins professionnelles, certaines recommandations doivent être respectées pour protéger les données qui peuvent être des données sensibles, soit au sens de leur caractère personnel et secret, soit parce qu'elles sont relatives à des travaux en cours qu'il convient de protéger pour pouvoir être, en temps utile, publiés et valorisés.

Tous les utilisateurs de l'Institut Curie, médecins, soignants, chercheurs, techniciens et administratifs, sont donc concernés par cette problématique de protection des données nécessaires à leur activité et qui constituent le patrimoine informationnel de l'Institut Curie.

Que l'on travaille au sein de l'Ensemble Hospitalier, du Centre de Recherche ou des Services Institutionnels, il faut veiller au respect des contraintes réglementaires préalablement à la mise en place un traitement de données dans le Cloud.

1.2 Données à caractère personnel

Selon la loi Informatique & Libertés, on appelle 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 la caractérise.

Exemples : un nom et une date de naissance, une date et un lieu de naissance, un n° de dossier (NIP), un n° histo, une adresse IP, une adresse email, un numéro de téléphone mobile, etc.

1.3 Données sensibles

Au sens de la CNIL, ce sont des données à caractère personnel qui font apparaître, directement ou indirectement : les origines raciales ou ethniques, les opinions politiques, philosophiques syndicales ou religieuses, la vie sexuelle, les infractions, les condamnations ou mesures de sûreté, le numéro de sécurité

sociale, des appréciations sur les difficultés sociales des personnes, des données biométriques, des données génétiques, des données relatives à la santé.

1.4 Traitement

Le terme « traitement » de données peut désigner le stockage, les échanges, l'archivage ou les calculs faits sur des données ou des documents. Il s'agit d'un terme consacré au niveau de la loi Informatique & Libertés et qui est repris dans la suite de ce document.

2. CNIL ou pas CNIL

Le traitement de données à caractère personnel ou sensible doit faire l'objet, selon le cas, d'une déclaration ou d'une demande d'autorisation préalables auprès de la CNIL. Lorsque le traitement se fait dans le Cloud des précautions particulières sont nécessaires, car quel que soit l'hébergeur, l'Institut Curie reste légalement responsable des données et de leur traitement.

L'exigence CNIL concerne toutes les activités de soins et un certain nombre d'activités de recherche.

Toute forme de traitement d'informations cliniques, biologiques, administratives ou sociales ou encore d'images incluant des noms de patients ou même uniquement des numéros de dossiers ou des numéros histologiques (données indirectement nominatives), doit faire l'objet d'une démarche auprès de la CNIL. A noter qu'il faut une demande d'autorisation préalable auprès de la CNIL quand ces données sont physiquement hébergées ou transmises hors de l'Union Européenne (par exemple sur un site dont les serveurs sont aux Etats-Unis ou en Asie).

Les patients auxquels les informations traitées peuvent être rattachées doivent être a minima informés des traitements effectués et, dans certains cas, donner leur consentement.

Cas particulier : le dossier patient de l'Ensemble hospitalier met en œuvre des traitements de données médicales sur des serveurs hébergés dans les locaux de l'hôpital. Ces traitements ont fait l'objet d'une déclaration auprès de la CNIL. Les patients en sont informés à travers le livret d'accueil qui leur est remis lors de leur première venue. Comme la tenue d'un dossier médical, dont le contenu est défini par le Code de la Santé Publique, est une obligation réglementaire pour les établissements de santé, le consentement des patients n'est pas requis pour ces traitements.

3. Datacenter et Patriot Act

Le cas du Patriot Act et du Cloud computing pose un problème particulier quant aux accès aux données sensibles (atteinte à la confidentialité et habilitations).

Depuis, 2001, les sites des entreprises américaines et des sociétés ayant des intérêts économiques aux USA sont soumis au « Patriot Act ». Cette loi est « extra-territoriale » et peut s'appliquer à des données hébergées dans les centres de données européens de ces sociétés. Il s'agit d'une loi américaine à vocation initiale de lutte contre le terrorisme et qui confère aux autorités des Etats-Unis le pouvoir d'accéder aux données présentes sur ces sites, que ce soit des données d'entreprises (base de données et fichiers divers) ou des données de particuliers (telles que des boîtes email privées ou des documents dans un espace de partage/d'échange de fichiers en ligne).

Ces dispositions s'opposent à certaines règles européennes sur la protection de la vie privée, et plus particulièrement à la réglementation sur l'accès aux données issues du domaine de la santé qui impose un accès strictement réservé aux personnes habilitées et ayant « besoin d'en connaître ».

A titre d'exemple on peut noter que :

Google publie ainsi tous les 6 mois dans son rapport de transparence le nombre de comptes Google surveillés dans le cadre du Patriot Act. En France de juillet à décembre 2012 : 2063 utilisateurs ont été surveillés, comme on peut le constater sur ce site :

http://www.google.com/transparencyreport/userdatarequests/FR/

Les règles de confidentialités de Dropbox indiquent « *Nous pouvons transmettre à des tiers externes à Dropbox les fichiers stockés dans votre Dropbox et les informations vous concernant si nous pensons, en toute bonne foi, que cette mesure est raisonnablement nécessaire […] pour respecter une loi ou une réglementation, ou répondre à une injonction de justice* »

4. Décret Hébergeur

En France, le stockage de données de la sphère santé est soumis au décret dit « décret hébergeur » depuis le 4 janvier 2006.

Au niveau de la loi française, les données recueillies ou produites à l'occasion d'activités de prévention, de diagnostic, de soin ou de recherche médicale peuvent être stockées, une fois le traitement déclaré à la CNIL, uniquement sur les serveurs d'une société ayant obtenu un agrément « d'hébergeur pour les données de santé ». Le décret n°2006-6 du 4 janvier 2006 définit les conditions d'agrément. La liste des hébergeurs agréés est disponible sur le site de l'ASIP Santé :

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

Par conséquent, mettre ce type de données sur un espace de partage et/ou stockage de fichiers en ligne autonome (Dropbox, Google Drive, Google Docs, SkyDrive, iCloud sont des sociétés soumises au Patriot Act, etc.) ou intégré à une solution plus packagée (logiciels d'analyse et d'archivage commerciaux en biologie : Ingenuity Variant Analysis, BaseSpace d'Illumina, Ion Reporter Software de Ion Torrent …) n'est pas conforme à la réglementation et engage la responsabilité de l'Institut Curie.

Seuls les établissements de santé qui hébergent, sur leurs serveurs locaux, les données cliniques et biologiques relatives à leurs propres patients sont dispensés de l'obtention de cet agrément.

Si un établissement de santé met en œuvre des services conduisant à stocker des données cliniques ou biologiques pour le compte d'autres structures et relatives à des patients qu'il ne prend pas directement en charge, il agit dans ce cas en tant qu'hébergeur de données et doit obtenir un agrément pour ce service d'hébergement.

5. Solution packagée dans le cloud

L'acquisition d'une solution packagée avec hébergement dans le Cloud doit faire l'objet d'une analyse de risques préalable, et si elle est retenue, doit comporter un contrat qui cadre les conditions de sécurité associées à sa mise en œuvre.

Certains fournisseurs proposent des systèmes (matériels + logiciels) sous forme de package. Au lieu d'être stockés sur des serveurs hébergés par l'Institut Curie dans ses datacenters, les résultats produits par ces systèmes sont ainsi envoyés et stockés dans le Cloud, chez un hébergeur qui est soit le fournisseur du système, soit l'un de ses sous-traitants.

Ce mode de fonctionnement, en apparence plus simple en termes d'exploitation, présente des risques juridiques et techniques importants et ne doit être choisi qu'après avoir analysé finement le contexte et défini contractuellement et techniquement les conditions de mise en œuvre. L'Institut Curie reste le « responsable du traitement » au sens de la loi Informatique & Libertés. Et en tant que responsable du

traitement, il encourt des sanctions pénales, notamment en cas de non-respect des dispositions de la loi « Informatique et libertés » du 6 janvier 1978 modifiée et/ou du décret hébergeur.

Pour chaque acquisition, si un stockage dans le Cloud est envisagé, il faut se poser les questions suivantes : les données sont-elles reliées ou reliables à des personnes ? Si oui, sont-elles associées à un identifiant qui permet de revenir à l'individu (si cette réversibilité est possible, alors on ne peut pas parler de données « anonymes »). Les données sont-elles sensibles ? Doivent-elles rester confidentielles dans le cadre de mes recherches, avant publication, valorisation, … ? L'hébergeur de ces données est-il agréé pour des données de santé ? Quel niveau de service est offert par la société qui héberge : engagement de mise à disposition 24/7 ? Sauvegarde quotidienne ? Quelle réversibilité est prévue si demain il est souhaité de réintégrer ces données en interne ou de solliciter un autre hébergeur ? Et la réversibilité est-elle techniquement possible ? Quel export des données est-on en droit de réclamer (quel format, quel délai vous est garanti pour l''obtention de vos informations, …) ? Quel personnel chez l'hébergeur peut accéder aux données ? Les données sont-elles chiffrées sur les systèmes de stockage de l'hébergeur ? Le site de l'hébergeur est-il sécurisé, autant au niveau de ses accès réseaux que des accès physiques ? L'hébergeur vous autorise-t-il à l'auditer au plan de la sécurité ? Etc.

Les Responsables Sécurité, la Direction des Systèmes d'Information de l'Ensemble Hospitalier, le Service Informatique du Centre de Recherche et la Direction Juridique doivent impérativement être sollicités en amont de tout projet impliquant un traitement dans le Cloud.

6. Messagerie électronique

Les boîtes email personnelles de type Gmail ou Yahoo mail ne doivent pas être utilisées à des fins professionnelles, notamment (mais pas seulement !) si elles servent à des échanges d'informations cliniques ou biologiques avec des professionnels extérieurs ou à des échanges avec des patients.

Lorsque nous ouvrons une boîte email personnelle chez un hébergeur tel que Yahoo ou Google, nous devons accepter les CGU (Conditions Générales d'Utilisation). Ces CGU comportent souvent des dizaines de pages, ce qui dissuade la plupart d'entre nous de les lire. Et nous les acceptons d'un clic, sans être bien conscients que Yahoo ou Google s'attribuent ainsi des droits de propriété et d'usage sur les messages contenus dans notre boîte email « privée ». Ils peuvent notamment inspecter les contenus de nos emails, non seulement pour afficher des publicités ciblées, mais aussi et surtout revendre ces informations à des sociétés tierces, par exemple.

Rappelons par ailleurs que les CGU de la version gratuite de Gmail accordent une licence pour un usage personnel uniquement **:** *« Google vous concède, à titre gratuit, une licence personnelle, non-cessible, non-exclusive et pour le monde entier, d'utilisation du logiciel qui vous est fourni par Google dans le cadre des Services. »*. Ce qui exclut une utilisation professionnelle, dont les services font partie d'une autre offre Google, payante celle-là.

Par conséquent, si nous envoyons via ce type de boîte email un compte-rendu médical ou un fichier contenant des résultats biologiques issus d'une plateforme ou d'une analyse, nous sommes pénalement sanctionnables. Et ce, à plusieurs titres : ces boîtes emails ne respectent ni le secret médical, ni la loi Informatique & Libertés, ni le « décret hébergeur » et sont le plus souvent soumises au Patriot Act. Il est donc interdit d'y faire circuler des informations professionnelles reliées ou reliables à des patients.

Il faut bien avoir à l'esprit que les données relatives à un patient sont couvertes par le secret médical et que l'Institut Curie n'en est que le dépositaire et l'exploitant. Nous sommes tenus de nous assurer du respect de ce secret médical ; à défaut, notre responsabilité peut être engagée.

De même, si l'on envoie via ce type de boîte email des documents professionnels relatifs à des travaux de recherche, par exemple, la confidentialité n'est nullement garantie. L'expéditeur perd le contrôle sur l'usage

qui sera fait de ses emails, et en cas de revente des informations à des sociétés tierces, cela peut conduire à la divulgation d'informations sur ses travaux en cours.

En matière de responsabilité, il faut utiliser, dans l'exercice de son activité professionnelle, les outils mis à notre disposition par l'Institut Curie qui est responsable de cette activité. Il faut donc utiliser les systèmes de messagerie de l'Institut Curie.

Rappelons, en outre, au plan technique, que l'email ne permet pas d'être certain de l'identité de ses interlocuteurs, qu'il circule en clair sur Internet (sauf si l'on recourt à des messageries sécurisées permettant le chiffrement et la signature électronique des messages), et qu'il n'est pas adapté à la traçabilité opposable et parfois obligatoire des échanges.

De plus, pour des raisons de visibilité et de réputation de l'Institut Curie, l'adresse d'une messagerie professionnelle ne doit pas être celle d'un fournisseur commercial.

Il faut enfin noter qu'un service gratuit comme Gmail ne fournit aucune garantie contractuelle en terme de disponibilité ou de fiabilité comme le précisent ses Conditions d'Utilisation : *« nous ne contractons aucun engagement concernant le contenu des Services, les fonctionnalités spécifiques disponibles par le biais des Services, leur fiabilité, leur disponibilité ou leur adéquation à vos besoins. Nous fournissons nos Services « en l'état ». »*

Attention : Si vous utilisez un smartphone avec lequel vous consultez votre boîte email professionnelle à l'Institut Curie et que, par ailleurs, vous activez par ailleurs la synchronisation de votre smartphone avec des services dans le Cloud, vous exposez vos emails professionnels aux risques précédemment évoqués.

7. Espaces collaboratifs

En dehors de tout contexte de données à caractère personnel, il est pratique de collaborer dans le cadre de projets via des outils en ligne. Oui, mais attention aux CGU.

Vous travaillez sur un projet avec des interlocuteurs externes à l'Institut Curie et avez besoin d'échanger des informations sur ce projet.

Attention, si vos fichiers sont sensibles et contiennent des informations susceptibles d'intéresser un projet concurrent, en les déposant sur un serveur en ligne vous perdez l'entière propriété et vous vous exposez à une exploitation commerciale de ces informations par votre hébergeur. Il faut également avoir à l'esprit que de nombreux « grands hébergeurs » se sont faits pirater et que des fuites d'information à grande échelle en déjà ont découlé ces dernières années.

Certains organismes tels que le CNRS ou l'INCA par exemple, ont mis en œuvre des espaces collaboratifs sécurisés qui permettent de répondre à un certain nombre de cas d'usage professionnels.

8. Réseaux Sociaux

Les réseaux sociaux sont des moyens riches d'échanges mais aussi des mines d'information pour les experts de la collecte de données et les hackers.

Les réseaux sociaux fonctionnent comme toutes les offres en ligne. C'est pourquoi il faut se limiter à y déposer des informations « sans risque » au plan personnel comme au plan professionnel.

Il ne faut donc pas y publier de données en relation avec des patients, ni d'information pouvant nuire à l'image ou révéler des informations confidentielles de l'Institut Curie. Sur un plan personnel, attention aux CV détaillés qui peuvent être réutilisés à des fins d'usurpation d'identité.

Attention également à ne pas mettre des informations qui dévoilent vos centres d'intérêt et pourraient être réutilisées contre vous. Ces dernières années, les opérations de phishing (hameçonnage) se multiplient. Il s'agit pour les attaquants de vous envoyer des emails contenant des liens vers des faux sites (imitation de site bancaire, par exemple). Ces sites piégés vous extorquent des données privées ou professionnelles qui sont ensuite revendues à des pirates capables de les exploiter. Ces derniers temps, les tentatives de phishing de masse ont cédé la place à du phishing ciblé. Les hackers font de « l'ingénierie sociale », c'est-à-dire qu'ils collectent des informations sur vous ou sur votre environnement professionnel grâce aux réseaux sociaux, notamment. Après ce profilage, ils peuvent vous adresser des emails ciblés avec une chance accrue de vous faire mordre à l'hameçon en vous faisant cliquer sur le lien contenu dans le mail.

Enfin, sur les réseaux sociaux, le droit à l'oubli, cher à la CNIL, n'existe pas. Si vous voulez effacer une information ou une photo que vous avez précédemment déposée, le réseau social ne vous le permet pas réellement puisque celles-ci restent conservées sur les serveurs des réseaux sociaux.

Vos données sont précieuses : collectées, décortiquées, compilées, analysées, ces données massives se révèlent très précieuses.

9. Stockage externalisé

Les logiciels de stockage et de partage de fichiers externalisés « en Cloud » offrent un moyen pratique d'accéder à des données en toutes circonstances. Leur usage dans un contexte professionnel ne peut toutefois se faire sans respecter certaines précautions à minima afin de protéger, en terme de sécurité et de confidentialité notamment, les données manipulées *(et donc l'activité du Centre de Recherche)*.

Avant de stocker toute information sur un système de stockage externalisé, nous vous recommandons de :

- **Ne pas stocker de données de santé** qui doivent **impérativement** être stockées par un hébergeur de données de santé agréé par le Ministère de la santé**,**

Plus généralement, **ne pas retranscrire de données à caractère personnel[1] ou de données sensibles[2]** qui, souvent, doivent faire l'objet de déclarations auprès de la Commission Nationale Informatique et Libertés (CNIL),

- **Etre particulièrement vigilant quant aux données confidentielles et/ ou des données stratégiques pour l'Institut Curie** car la confidentialité sur des espaces de stockage externalisés n'est pas garantie. Les mécanismes de partage en cascade ne permettent pas de maitriser réellement la portée de la diffusion des données scientifiques et autres,
- **Ne pas installer le logiciel de stockage externalisé sur des ordinateurs qui n'ont pas été configurés par l'Institut Curie**, et qui ne bénéficieraient pas des protections en vigueur au Centre de Recherche en termes de sécurité informatique (chiffrement des media),
- Garder à l'esprit que **toute altération du système de stockage externalisé (suppression et/ou modification de fichiers) sera répercutée sur le serveur et tous les postes distants**. Par ailleurs, un **logiciel malveillant sur un poste distant pourrait librement accéder aux données, les supprimer, altérer, verrouiller le logiciel** et ainsi fausser l'information accessible sur le système de stockage et de partage externalisé,
- **Sauvegarder les données régulièrement**, en cas de panne, perte ou vol d'ordinateur, cessation de la licence d'utilisation du système de stockage externalisé… A titre d'exemple, Dropbox n'assure pas la sauvegarde des données et elles peuvent être définitivement perdues. Nous recommandons donc de ne pas utiliser le système de stockage externalisé comme un espace d'archivage mais comme un **espace temporaire d'échange de fichiers**.

En cours d'utilisation de l'espace de stockage et de partage des fichiers :

Prévenir systématiquement et rapidement en cas de départ d'un collaborateur de l'Institut Curie pour qui il conviendrait de supprimer le « compte utilisateur ».

10. Recommandations

- Respecter le contexte réglementaire strict : démarches CNIL, appel à un hébergeur agréé en cas de stockage de données cliniques et biologiques.
- Garder en mémoire le Patriot Act et le fait que toute donnée hébergée sur des serveurs américains deviennent consultables par des tiers.
- Prendre des précautions dans les usages de services en ligne. Etre vigilant sur les conditions d'hébergement relatives à : la sécurité du système hébergeur, la propriété et l'exploitation de l'information, à la réversibilité de l'externalisation, aux droits d'accès à l'information.
- S'assurer du respect du secret médical lié à toute donnée clinique ou biologique ;
- Solliciter les responsables sécurité de l'information et le service juridique en amont de tout projet pour lequel il est envisagé de recourir à un système dans le Cloud ;
- Séparer clairement les usages entre sa boîte email professionnelle hébergée à l'Institut Curie et sa boîte email personnelle potentiellement dans le Cloud ;
- Faire un usage averti des espaces collaboratifs et des réseaux sociaux ;
- Avoir à l'esprit que les services en ligne gratuits se rémunèrent sur les informations obtenues ;

Paris, le 2 février 2011

INFORMATION A L'ENSEMBLE DU PERSONNEL TRAVAILLANT DANS LES LOCAUX DE L'INSTITUT CURIE , SECTION DE RECHERCHE SUR LA GESTION DES COUTS DE TELEPHONIE

Conformément à la réglementation de la CNIL notre système de traitement automatisé de données à caractère personnel mis en œuvre dans le cadre de l'utilisation des services de téléphonie a été enregistré auprès de cet organisme sous le n° 1247567.

Nous souhaitons rappeler les dispositions qui s'appliquent en matière de contrôle des consommations téléphoniques et d'utilisation des données personnelles issues de notre système de téléphonie .
Nous rappelons également que l'utilisation de la téléphonie est destinée à un usage professionnel et que seul un usage limité à titre personnel peut être toléré.

TAXATION TELEPHONIQUE

Objet
Nous disposons à Orsay et à Paris d'autocommutateurs dont le but est de permettre de répartir les frais téléphoniques analytiquement sur les différentes unités et les différents services et de maîtriser les coûts liés à la consommation des services téléphoniques.

Modalités
Les listings dont nous disposons nous permettent de connaître le coût par numéro de poste et utilisateurs(s) rattaché(s) et d'effectuer la répartition analytique par unité et/ou département/ service.

1) Chaque trimestre il sera communiqué aux Directeurs d'unités et/ou de départements un listing reprenant le coût par poste des communications téléphoniques de son unité ou de son département qui lui seront refacturées sur la base de ce listing.

Ce document ne fait pas apparaître le détail des communications.

2) En cas de coût excessif constatée à l'occasion de l'établissement des relevés non détaillés les supérieurs hiérarchiques des personnels concernés peuvent demander la liste des numéros

appelés à partir d'un poste qui pourra également être transmise à la GRH en cas d'utilisation manifestement abusive.
Lorsque les relevés justificatifs sont établis les quatre derniers numéros sont occultés de façon à rester en conformité avec la Loi Informatique et libertés.
Cette liste sera également communiquée au titulaire du poste téléphonique .

3)Usage manifestement abusif

Toutefois la Commission Informatique et libertés admet que l'intégralité des numéros appelés depuis les postes de l'entreprise puisse être éditée par l'entreprise ou l'organisme privé en cas d'utilisation manifestement abusive, dans le cas où :

- un remboursement est demandé aux employés pour les services de téléphonie, utilisés à titre privé, lorsque le montant est contesté par le salarié auquel il se rapporte,
- une utilisation manifestement anormale au regard de l'utilisation moyenne constatée au sein de l'entreprise ou de l'organisme privé nécessite un relevé justificatif complet établi de manière contradictoire avec l'employé concerné.

L'intégralité des numéros sera communiquée exclusivement :

- à la personne concernée
- au Directeur de la section de recherche, au Directeur adjoint , aux directeurs de département ou de service concernés et aux directeurs d'unités INSERM ou CNRS le cas échéant .
- à la Direction du Personnel

Ces numéros ne seront pas communiqués à d'autres salariés dans le respect des recommandations de la Commission Informatique et Libertés.

En cas d'usage abusif des lignes téléphoniques professionnelles à des fins privées, les intéressés en seront informés ; ils disposeront d'un droit d'accès et de rectification éventuelle aux informations qui leur seront fournies.

Des sanctions pourront être prises contre les intéressés si nécessaire dans le respect des règles légales en vigueur.

La durée de conservation des données relatives aux numéros de téléphone appelés ne dépassera pas une année

Les représentants du personnel peuvent, s'ils le souhaitent, disposer d'une ligne téléphonique non connectée à l'autocommutateur de façon à ce que l'employeur ne puisse identifier en aucune façon les correspondants appelés par eux dans le cadre de leur représentation salariale : ils doivent en faire la demande auprès du Directeur adjoint.

Corinne CUMIN
Directeur adjoint du Centre de Recherche

Compte informatique (adresse électronique) : procédure de maintien ou de fermeture

Cette procédure est valable que le dossier de la personne soit renseigné dans le logiciel RH (salariés, stagiaires, Agents CNRS/INSERM,…) ou bénéficie d'une adresse électronique en qualité d' "extérieur".