RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inserm
La science pour la santé
From science to health

Charte de l'*Utilisateur* des ressources informatiques de l'Inserm

Ce texte définit un cadre minimal d'utilisation des systèmes d'information et réseaux informatiques de l'Inserm. Il s'applique de manière unique à tous les *Utilisateur*s, dès lors qu'ils utilisent un Système d'information de l'Inserm.

L'objectif de cette charte est d'assurer l'accès à ces Systèmes d'information dans des conditions optimales et claires pour tous.

Elle est disponible librement et accessible à toutes les personnes concernées sur le site https://pro.inserm.fr.

L'accès aux systèmes d'information est subordonné à l'acceptation de cette charte. Le non-respect de la charte peut entrainer la suspension de l'autorisation d'accès délivrée à l'*Utilisateur*.

Pour tout renseignement complémentaire, les *Utilisateur*s peuvent s'adresser, selon le cas, au responsable informatique de la délégation dont ils dépendent, au délégué à la protection des données, ou au responsable de la sécurité des systèmes d'information de l'Inserm.

1 - Définitions

On désigne sous le terme « *Entité* » les structures créées par l'Inserm pour l'accomplissement de ses missions, telles que les Unités de Recherche, les Équipes, ainsi que les Départements et Services administratifs.

On désigne de façon générale sous le terme « *Ressources informatiques* », les moyens informatiques de calcul ou de gestion sous responsabilité de l'Inserm, qu'ils soient locaux ou accessibles à distance, ainsi que les services de réseau sous responsabilité de l'Inserm permettant la communication locale ou distante.

On désigne par « *Services Internet* », les services offerts par des organismes et sociétés tierces, qu'ils soient ou non liés par contrat avec l'Inserm.

On désigne sous le terme « *Utilisateur* », les personnes ayant accès ou utilisant les ressources informatiques et services Internet au sein d'une entité de l'Inserm. Le terme recouvre non limitativement les agents de l'Inserm, les personnels associés, les stagiaires, les étudiants ou les prestataires externes.

On désigne sous le terme « *Administrateur* » les personnes assurant les fonctions de gestion, de supervision ou de maintenance des ressources informatiques ou des accès aux services internet.

On désigne sous le terme de « *Matériel* » les équipements informatiques (postes, portables, tablettes, mobiles, dispositifs matériels d'authentification).

2 - Conditions d'utilisation des Ressources informatiques

L'utilisation des *Ressources informatiques* et l'usage des *Services Internet* ne sont autorisés que dans le cadre de l'activité professionnelle des *Utilisateurs.*

Pour un agent Inserm, la notion d'activité professionnelle s'apprécie au regard notamment des dispositions du Code de la Recherche ou du Décret 83-975 relatif à l'organisation et au fonctionnement de l'Inserm.

L'utilisation des *Ressources informatiques* de l'*Entité* et la connexion d'un équipement, quel qu'il soit, sur le réseau entrant dans le cadre des *Ressources informatiques* sont en outre soumises à autorisation.

Ces autorisations sont, sauf organisation spécifique de l'Entité, délivrées sous l'autorité du directeur de l'*Entité*, sont strictement personnelles et nominatives et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles sont communiquées par l'Entité à l'Administrateur pour suite à donner.

Ces autorisations peuvent être suspendues ou retirées à tout moment par l'autorité l'ayant délivrée.

L'*Entité* pourra en outre prévoir des restrictions d'accès spécifiques à son organisation interne.

3 - Matériel

Pour les besoins de son activité professionnelle, des Matériels (postes, portables, tablettes, mobiles, dispositifs matériels d'authentification, etc.) sont susceptibles d'être fournis par l'Inserm à *l'Utilisateur*. Ces Matériels, ici qualifiés de Matériel professionnel, sont destinés exclusivement à l'activité professionnelle. L'*Utilisateur* ne doit pas installer des logiciels à usage personnel sur ces Matériel professionnel, même s'il en a la possibilité technique. Toute installation de logiciels ou mise à jour nécessite de solliciter l'Administrateur.

Ces Matériels professionnels sont susceptibles d'être monitorés ou pris en charge par l'Administrateur notamment pour des raisons de sécurité. L'*Utilisateur* sera informé au préalable de cette intervention. Les personnels de l'Administrateur en charge de ces opérations, notamment de maintenance ou de contrôle, sont soumis à une obligation de confidentialité. Ils ne peuvent en aucun cas communiquer à un tiers les données accédées sur les Matériel professionnel dans le cadre de ces opérations de contrôle et maintenance.

Néanmoins, il est rappelé qu'en application de l'article 40 du Code de procédure pénale, tout fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.

Lorsque cela est nécessaire, l'*Utilisateur* doit s'assurer de la protection des données sur ces équipements, en veillant à leur sécurisation ou à la sauvegarde de ceux-ci. Si le Matériel professionnel ne lui semble pas conforme, il doit en porter connaissance à l'Administrateur.

Lorsqu'un Matériel contient des données sensibles, celles-ci doivent être sécurisées par un dispositif de chiffrement. L'Administrateur est chargé d'installer ces dispositifs de chiffrement sur le Matériel professionnel.

L'utilisation des *Ressources informatiques* doit se faire via ces Matériels professionnels.

L'utilisation du Matériel personnel est interdite sauf impossibilité, dûment justifiée, d'utiliser un Matériel professionnel et sous réserve d'une autorisation préalable du directeur de l'*entité* et d'une vérification par l'Administrateur de la conformité du Matériel personnel avec les règles et normes en vigueur à l'Inserm.

Les Matériels professionnels doivent être restitués à la fin de l'activité pour laquelle ils ont été fournis.

4 - Contrôle d'accès

L'accès aux *Ressources informatiques* non publiques par un *Utilisateur* est soumis à un contrôle d'accès via des moyens appropriés : mots de passe, certificats numériques, dispositifs matériels, etc. Ces moyens d'accès sont strictement personnels et nominatifs et ne peuvent en aucun cas être divulgués ou cédés, même temporairement, à une autre personne, collègue, tiers ou membre de la famille.

Chaque *Utilisateur* est responsable de ces moyens d'accès et doit en assurer la confidentialité. Les moyens physiques doivent être protégés contre le vol, les moyens logiques doivent être stockés de manière sécurisée, et les mots de passe ne doivent pas être notés ou enregistrés sur un support non sécurisé.

En cas de perte ou divulgation, l'*Utilisateur* doit informer sans délai les *Administrateurs* pour suite à donner (le cas échéant, afin d'invalider ou remplacer le moyen d'accès concerné, si l'*Utilisateur* ne l'a pas fait de son coté).

L'*Utilisateur* n'est pas autorisé à communiquer son mot de passe lui permettant d'accéder au Matériel Professionnel ou aux Ressources informatiques. Néanmoins, lorsque l'*Utilisateur* doit, à titre exceptionnel, pour besoin de service et de façon temporaire, communiquer un mot de passe, il doit s'assurer que la personne à qui il le communique est dument autorisée par le directeur de l'*Entité*. L'*Utilisateur* devra ensuite et dans les plus brefs délais changer son mot de passe.

Les moyens d'authentification utilisés à titre professionnel pour les *ressources informatiques* de l'Inserm ne doivent ne pas être réutilisés pour un autre cadre. Chaque *Utilisateur* doit veiller à ne pas réutiliser ses mots de passe ou certificats numériques professionnels Inserm dans tout autre cadre sur des *services Internet*.

Lorsqu'il utilise un mécanisme de récupération de mots de passe ou certificats numériques de l'Inserm, l'*Utilisateur* doit s'assurer que celui-ci est sécurisé, notamment s'il passe par un *service Internet* personnel.

5 - Conditions d'utilisation des Ressources informatiques

L'utilisation des *Ressources informatiques* doit être rationnelle et loyale afin d'en éviter notamment leur saturation ou leur détournement.

En particulier, un *Utilisateur* :

- Doit appliquer les éventuelles recommandations de sécurité en vigueur au sein de l'*entité* à laquelle il appartient ;
- Doit suivre les éventuelles règles en vigueur au sein de l'*entité* pour toute installation de logiciels ;
- Doit appliquer les règles en vigueur pour l'ensemble de l'Inserm, dont la PSSI ;
- Doit signaler à l'Administrateur toute tentative de violation de son compte et de façon générale toute anomalie qu'il peut constater ;
- Ne doit pas mettre à la disposition d'*Utilisateurs* non autorisés un accès aux *ressources informatiques*, à travers les Matériels dont il a l'usage ;
- Ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;
- Ne doit pas mésuser ou abuser des droits qui lui sont attribués, en ce compris la lecture, la modification, la copie ou la destruction de données dès lors que ces actions ne sont pas légitimes ;
- Doit verrouiller son poste de travail lorsqu'il quitte son poste de travail, y compris pour un court instant, afin d'éviter tout mésusage des *ressources informatiques* ou *Services Internet* accessibles.

L'utilisation des *ressources informatiques* doit être licite.

En particulier :

- Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par l'*Administrateur* ;
- Il est interdit de contourner les restrictions d'utilisation d'un logiciel ;
- L'installation sur un système informatique mis en œuvre par l'Inserm d'un logiciel dont le droit d'usage est acquis à titre privé par un *Utilisateur* n'est pas autorisée ;
- L'*Utilisateur* doit se conformer aux termes des licences des logiciels utilisés à l'Inserm qui lui sont communiqués ;
- L'*Utilisateur* s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux (internes ou extérieurs à l'Inserm) que ce soit par des manipulations anormales des ressources, ou par l'introduction de logiciels malveillants connus sous le nom générique de virus, chevaux de Troie, bombes logiques ou assimilés ;
- L'*Utilisateur* s'engage à ne pas constituer des fichiers ou créer des traitements de données à caractère personnel, tels que définis par le Règlement général sur la protection des données, sans en avoir obtenu l'autorisation préalable écrite du directeur de l'*entité*. L'ensemble des traitements et fichiers doit être versé au registre des traitements du responsable légal de traitement.

Ces conditions s'appliquent sans préjudice des dispositions légales et réglementaires en vigueur applicables et notamment :

- Le Code de la propriété intellectuelle ;
- Le Code général de la fonction publique dont les articles relatifs aux obligations générales applicables aux agents publics (Articles L121-1 à L121-11) ;
- Le Code pénal, dont les articles 323-1 et suivants relatif aux atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8) ;
- La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dénommé « Règlement général sur la protection des données » ou le « RGPD »).

6 - Utilisation des services Internet

L'*Utilisateur* ne doit faire usage des *services Internet* auxquels il accède grâce au moyen des *Ressources informatiques* de l'Inserm ou du *Matériel professionnel, que* pour les besoins exclusifs de ses activités professionnelles et que dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

7 - Usage de la messagerie et des services de travail collaboratif par les agents

Un accès à la messagerie de l'Inserm et à d'autres outils de travail collaboratif est susceptible d'être ouvert à l'*Utilisateur*.

Cet accès est accordé pour les seuls besoins de l'activité professionnelle.

Il est toléré une vie privée résiduelle associée à la messagerie, mais tout message ou document à usage personnel doit être clairement identifié comme tel par la mention « privé », et leur nombre limité.

Chaque *Utilisateur* prendra l'attache de l'*Administrateur* afin d'organiser et mettre en œuvre les moyens nécessaires pour la conservation des messages considérés comme indispensables ou simplement utiles comme élément de preuve. Il en sera de même si ceux-ci sont conservés hors des

serveurs de messagerie (afin que ces archives soient sauvegardées).

Les *Utilisateurs* de la messagerie doivent veiller à ne pas mésuser celle-ci, notamment via l'envoi de messages de masse.

S'agissant des pièces jointes volumineuses, l'*Utilisateur* doit privilégier le transfert de données via des *ressources informatiques* adaptées plutôt que via la messagerie.

Lorsque les documents ou messages sont particulièrement sensibles l'*Utilisateur* prendra l'attache de l'*Administrateur* afin que ces documents ou messages soient chiffrés préalablement.

L'utilisation de la messagerie ou d'un service de travail collaboratif pour des données classifiées (Diffusion Restreinte) n'est possible qu'en liaison avec un mécanisme de chiffrement agréé par l'ANSSI. L'utilisation de la messagerie ou des services de travail collaboratif pour les données classifiées de degré supérieur n'est pas autorisée. L'*Utilisateur* se rapprochera de l'*Administrateur* s'il est amené à traiter des données classifiées afin de s'assurer que cet usage est conforme aux normes et recommandations en vigueur.

Il n'est pas autorisé de transférer messages et contenus vers des services de messagerie ou de travail collaboratif dépendant d'organismes ou sociétés externes, exception faite des tutelles ou établissement de recherche dont dépends l'*Utilisateur* ou son Entité. Une attention toute particulière doit être portée sur les transferts automatisés (synchronisation, redirection de messagerie). L'*Utilisateur* se rapprochera de l'Administrateur pour traiter ce point.

L'usage d'outils grand public pour la messagerie ou le travail collaboratif est soumis à dérogation explicite et écrite du directeur de l'*Entité* dont dépend l'*Utilisateur* et autorisation préalable de l'*Administrateur*.

Ces dérogations ne sont nécessaires que pour les documents et messages sous la responsabilité de l'*Utilisateur*. Le travail collaboratif et les échanges avec des tiers hors Inserm peut se faire sous la responsabilité de ce tiers, avec les outils ou messageries dudit tiers.

8 - Création de fichiers

Les fichiers détenus et/ou créés par un *Utilisateur* sont présumés avoir un caractère professionnel.

Par dérogation à l'usage à des fins professionnelles, toute utilisation de l'outil informatique à des fins personnelles doit être résiduelle, tant dans la fréquence que dans la durée, conformément aux conditions et limites définies ci-dessous.

A ce titre, les *Utilisateur*s doivent classer les fichiers relevant de leur vie privée dans un dossier portant le titre de « personnel » ou « privé », lequel ne devra en aucune manière être stocké sur un emplacement communautaire (Intranet, espace collaboratif, serveur etc.).

En toute hypothèse, l'utilisation à des fins personnelles des outils informatiques est limitée à un usage raisonnable ; il ne doit, en aucune manière, perturber le bon fonctionnement du service et des moyens informatiques.

9 - Traçabilité – Filtrage

Pour satisfaire aux obligations légales qui incombent à l'Inserm, tenant à sa capacité à :

- apporter la preuve, le cas échéant, du bon usage professionnel des systèmes d'information mis à la disposition de l'*Utilisateur* ;
- à prévenir tout usage illicite de ces systèmes d'information.

Il est procédé, dans le respect de l'information des personnes concernées et de la loi Informatique et libertés du 6 janvier 1978 modifiée et du Règlement européen 2016/679 du 27 avril 2016 à la mise en place :

- d'outils de traçabilité (journaux de connexions) de l'ensemble des systèmes d'information ;

- d'outils de filtrage (filtrage des contenus, des URL, protocolaire, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre ou d'interdire l'accès à internet ou à certaines catégories de sites internet.

- Dans le respect des principes de transparence et de proportionnalité, l'*Utilisateur* est informé que les dispositifs de sécurité informatique (pare-feu, systèmes de contrôle des accès, etc.) mis en place par l'Inserm enregistrent des traces et que des systèmes de filtrage sont mis en place, en particulier :

- pour les messages entrants et sortants avec un contrôle antiviral ;
- pour les messages dont la taille ou la liste de destinataires est trop importante ;
- pour les messages en provenance ou à destination d'un *Utilisateur* ou d'un serveur de messagerie électronique de nature manifestement hostile (envoi massif de messages, harcèlement d'un *Utilisateur*, etc.) ;
- pour bloquer sur la base d'une liste de « mots-clés » des messages ou l'accès à des sites non autorisés ;
- plus généralement, tout filtrage nécessaire pour préserver la sécurité du système d'information peut être mis en œuvre.

Le fonctionnement de ces systèmes de filtrage ressort de la compétence des *Administrateurs*.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

10 - Contrôle des Systèmes d'Informations

L'Inserm possède le droit de contrôler l'utilisation qui est faite des moyens informatiques par les *Utilisateur*s dans les limites prévues par la loi et la jurisprudence, et après information préalable des *Utilisateur*s.

Les personnes habilitées de la Direction des Systèmes d'Information, dûment mandatées pour mener ces démarches, garderont confidentielles les informations qu'ils pourraient être amenés à connaître à cette occasion.

A ce titre, les *Utilisateur*s sont informés que les personnes habilitées de la Direction des Systèmes d'Information qui doivent veiller au fonctionnement normal et à la sécurité des réseaux et systèmes informatiques sont conduits, de par leurs fonctions, à avoir accès à l'ensemble des informations relatives aux *Utilisateur*s (messages, connexion à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail, exception faite des documents sur-chiffrés pour raison de confidentialité.

Néanmoins, ces derniers sont tenus à une obligation de discrétion renforcée et ne peuvent utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

Des contrôles systématiques ou par échantillonnages ou en fonction d'éléments indiquant une utilisation hors norme peuvent être réalisés sur l'ensemble des Systèmes d'information mis à la disposition de l'*Utilisateur*, à n'importe quel moment et ce afin d'effectuer tout acte de protection des Systèmes, notamment pour se prémunir contre une utilisation non conforme pouvant notamment porter préjudice à l'Inserm.

L'Inserm se réserve dans le cadre de ces missions notamment le droit :

- de vérifier le trafic informatique entrant et sortant (durée de connexion, sites visités, heures des visites, éléments téléchargés…), ainsi que le trafic transitant sur le réseau interne ;
- de vérifier certains types de contenu qui sont souvent à l'origine d'incidents (problèmes espace disque, encombrement du réseau, diffusion en chaîne, « cookies », etc.) ;

- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
- de contrôler l'origine licite des logiciels installés ;
- de filtrer les adresses électroniques (URL) des sites non autorisés ;
- de prendre connaissance des copies de tous les mails professionnels sur demande de la direction générale, de la direction des ressources humaines, etc. ;
- de conserver des fichiers de journalisation des traces de connexion globales pour une période n'excédant pas six mois ;
- de contrôler l'usage de la messagerie, en terme de volume/nombre de messages échangés, taille des messages, format des pièces jointes, quantité d'espace disque utilisé, analyse des messages (sélection de mots à caractère pornographique, raciste, etc.) ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

En cas de faisceau d'indices laissant supposer qu'un *Utilisateur* met en cause les intérêts ou la sécurité de l'Inserm en ne respectant pas les règles instituées par la présente charte, la Direction des Systèmes d'Information se réserve le droit de fournir à la Direction des Ressources Humaines, sur sa demande écrite et motivée, les traces individuelles des connexions incriminées sur une période n'excédant pas six mois.

En outre, en cas d'incident, l'Inserm se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;
- vérifier le contenu des disques durs des ressources du système d'information attribuées aux *Utilisateur*s ;
- procéder à toutes copies utiles à faire valoir ses droits.

La Direction des Systèmes d'Information exerce un contrôle des services informatiques sur les durées de connexion, les sites les plus visités dans le cadre de la mission de protection des systèmes informatiques. En cas de perturbation, induite par l'apparition intempestive d'alertes suite à tentatives d'infection des systèmes à l'aide de virus informatiques, la Direction des Systèmes d'Information est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

En cas de non-respect de la présente charte par un *Utilisateur*, la Direction des Systèmes d'Information se verra dans l'obligation d'avertir le supérieur hiérarchique de l'*Utilisateur* pour que celui-ci décide de la suite à donner.

Suivant la gravité des faits, les droits d'accès de l'*Utilisateur* concerné pourront être suspendus.

Tout logiciel installé illicitement ou tout fichier suspect sera supprimé par les intervenants de la Direction des Systèmes d'Information dès le constat de leur présence sur le poste de travail.

11 - Traitement des données à caractère personnel

L'Inserm, responsable de traitement, met en œuvre des traitements de données à caractère personnel pour la gestion de son système d'information à l'égard de l'ensemble des *Utilisateur*s. La base légale du traitement est l'intérêt légitime.
Ces traitements permettent notamment d'assurer :

- la gestion et le contrôle de l'utilisation des systèmes d'information ;
- le suivi et la maintenance des moyens informatiques ;
- la définition des autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement du système d'information ;
- la sécurité des moyens informatiques et des systèmes d'information ;
- la gestion de la messagerie électronique professionnelle.

Des données à caractère personnel concernant les *Utilisateur*s pourront également être traitées dans le cadre de la gestion des dossiers sur lesquels interviennent les *Utilisateur*s. En outre, des logs de connexion aux outils informatiques pourront être collectés pour des raisons de sécurité.

Les données collectées sont indispensables à ces traitements et sont destinées aux services concernés de l'Inserm, ainsi que, le cas échéant, à ses sous-traitants ou prestataires.

Les données collectées sont susceptibles d'être conservées pendant toute la durée de la relation contractuelle augmentée de la durée des prescriptions légales.

Des durées plus courtes peuvent parfois être appliquées en fonction de la finalité des traitements comme pour les logs de connexion aux outils informatiques qui sont conservés pendant 1 an.

En application de la législation en vigueur, l'*Utilisateur* dispose d'un droit d'accès, de rectification ou d'effacement, de limitation du traitement de ses données, d'un droit d'opposition au traitement, d'un droit à la portabilité de ses données ainsi que du droit de définir des directives relatives au sort de ses données après son décès, qui s'exercent par courrier électronique à l'adresse dpo@inserm.fr ou par courrier postal à l'attention du délégué à la protection des données, à l'adresse suivante : 101 rue de Tolbiac, 75013 Paris.

L'*Utilisateur* dispose enfin du droit d'introduire une réclamation auprès de la CNIL.

12 - Application

La présente charte s'applique à l'ensemble des agents de l'Inserm tous statuts confondus, d'une part, et d'autre part à l'ensemble des personnes extérieures, permanentes ou temporaires, utilisant les *ressources informatiques* de l'Inserm.

Elle sera en outre signée par toutes personnes accueillies à l'Inserm et ayant accès audit système.

NOM / PRENOM :

DEPARTEMENT :

DATE :

SIGNATURE :
(Précédée par la mention "Lu et approuvé, bon pour accord")

Fait à Paris, le 06/10/2023

Le président Directeur Général
Didier Samuel

Pour le PDG, et par délégation,

Damien Rousset
Directeur Général Délégué à l'Administration