Article 1 – Objet
Les présentes Conditions Particulières ont pour objet de définir les modalités et conditions dans lesquelles CompuGroup Medical France (GMF dans la suite du document) fournit à l'Abonné les services proposés dans le cadre du service « Fortidata - Sauvegarde en ligne » (le « Service »).

Article 2 - Formation du Contrat
Le contrat conclu entre l'Abonné et CGMF (le « Contrat ») est constitué des Conditions Générales de CGMF, des présentes Conditions Particulières du Service, du formulaire d'abonnement dûment complété et signé par l'Abonné, des tarifs et de la brochure commerciale de CGMF décrivant les caractéristiques du Service.

Article 3 - Définitions
Dans le présent document, les termes et expressions commençant par une majuscule, au singulier ou au pluriel, ont le sens qui leur est donné par les Conditions Générales.

Article 4 - Service
Fortidata - Sauvegarde en Ligne est une solution pour sauvegarder automatiquement les fichiers et les données médicales sensibles vers des infrastructures opérées et hébergées par CGMF et ce via une connexion Internet haut-débit.

Le service « Fortidata - Sauvegarde en ligne » est constitué par
- ✓ Un logiciel installé sur le poste du client permettant l'exécution des tâches de sauvegarde (licence logicielle mono-poste).
- ✓ Un abonnement mensuel permettant l'accès par l'Abonné à un espace de sauvegarde externe et mutualisé, dont la capacité est déterminée par l'Abonné lors de la souscription au Service, et peut être modifiée à tout moment.
- ✓ L'accès à un site Web lui permettant de visualiser l'état de ses sauvegardes, et d'effectuer des restaurations ponctuelles de fichiers sans disposer du logiciel sur son poste.

Dans le cadre d'un cabinet multi-postes, le logiciel est installé sur un serveur du cabinet afin de centraliser les sauvegardes de l'ensemble des postes.

Ce service est souscrit pour une durée définie dans l'article 12.

Article 5 - Activation du service - Accès à Internet
Suivant la réception par CGMF de la souscription d'un nouvel Abonné, celui-ci reçoit par courrier électronique un lien permettant le téléchargement du logiciel de sauvegarde. Une fois le logiciel installé et éventuellement paramétré, l'accès au service est possible grâce aux identifiants que CGMF a communiqué à l'Abonné dans son courrier ou courriel de bienvenue.

Le Client doit également fournir son numéro de téléphone mobile (et éventuellement en secours un second numéro de GSM ou une adresse mail) qui sera utilisé par CGMF pour l'envoi d'un code unique lors des demandes de restauration des données sauvegardées (système OTP – « One Time Password »).
Le Client renseigne également une adresse mail par défaut qui servira pour recevoir les rapports d'exécution des sauvegardes et restaurations.

Le Service est accessible à partir d'un ordinateur connecté à un réseau de télécommunication compatible avec le service d'accès à Internet. L'ordinateur de l'Abonné doit répondre à la configuration minimale visée sur la documentation de l'offre. Les protocoles de communication utilisés sont ceux en usage sur Internet. A ce titre, l'abonné s'engage à respecter les modalités d'utilisation du logiciel fourni.

Article 6 - Accès au service
L'accès au Service est subordonné aux conditions cumulatives suivantes :
- ✓ Présence d'un raccordement Internet de type xDSL (ADSL, SDSL…), et à la souscription au Service.
- ✓ Compatibilité technique de l'équipement informatique de l'Abonné. Pour ce faire, l'ordinateur de l'Abonné doit répondre aux caractéristiques spécifiées par CGMF.

CGMF ne pourra, en aucun cas, être tenue responsable d'une incompatibilité technique entre le logiciel et le matériel de l'Abonné.
L'accès au service est possible à la date de réception par l'Abonné des éléments personnels d'identification, à savoir : identifiant, mot de passe et adresse du serveur, la robustesse de ce mot de passe est assurée par une longueur d'au minimum 8 caractères avec la présence obligatoire d'au moins une majuscule, une minuscule et un chiffre ou caractère spécial.

Article 7 - Utilisation du service
Le Service doit être utilisé conformément aux lois et réglementations en vigueur. Le service ne peut en aucun cas être utilisé dans des lieux publics ou espaces commerciaux à usage public. Ceci exclut en particulier son usage sur des bornes en libre-service, espaces de type « Cyber », salons de démonstrations temporaires ou permanents, à moins qu'il ne soit expressément autorisé par CGMF.

Article 8 - Passphrase ou phrase secrète
Lors du paramétrage du logiciel, l'utilisateur est invité à saisir une phrase secrète qui sert de base au chiffrement des données qui seront stockées sur les infrastructures de CGMF. L'utilisateur est informé de ce qu'en cas de perte de cette phrase secrète, seul le médecin de l'hébergeur aura la possibilité de restaurer vos données sauvegardées dans le cadre d'une procédure facturée. L'utilisateur devra donc s'assurer de retenir cette phrase secrète aussi longtemps qu'il se doit, la robustesse de cette passphrase est assurée par une contrainte de saisie d'une longueur d'au minimum 8 caractères avec la présence obligatoire d'au moins une majuscule, une minuscule et un chiffre ou caractère spécial

Article 9 - Responsabilité des sauvegardes
L'Abonné définit une politique personnelle de sauvegarde automatique ou manuelle et est le seul garant de cette dernière. Cette politique doit inclure la liste des données à sauvegarder et la planification des sauvegardes dans le temps. Certaines données ne peuvent être sauvegardées que sous certaines conditions techniques (ex. fichier de base de données d'un logiciel de gestion patient nécessitant l'arrêt de ce logiciel pour effectuer la sauvegarde). Il est de la responsabilité du client de vérifier ces conditions.

De plus, CGMF conseille de vérifier le bon déroulement des sauvegardes régulièrement en visualisant les journaux sur le logiciel ou sur le serveur Web. De plus, il est recommandé de procéder régulièrement à des tests de restauration et de bonne réutilisation des données sauvegardées.

La technologie de sauvegarde des fichiers ouverts utilise les « clichés instantanés », également nommés VSS, de Microsoft. Leur utilisation ainsi que leur adéquation par rapport aux applicatifs clients utilisant ou verrouillant des fichiers n'est pas du domaine de responsabilité du RSS ni de son domaine de support technique.

Article 10 - Propriété des Données
Les Données sauvegardée et stockées par CGMF pour le compte du Client ou à l'initiative de celui-ci sont et demeurent la propriété du Client.

Article 11 – Modification ou évolutions techniques
CGMF se réserve le droit de faire évoluer son infrastructure informatique, sans altérer le Service tel qu'il existe au moment de la souscription, afin de garantir la qualité, la performance et la sécurité des services délivrés.

CGMF mettra tout en œuvre pour que ces évolutions aient le minimum d'impacts pour le Client, notamment en matière de disponibilité du Service d'intégrité des données sauvegardées.

Article 12 - Durée du contrat
Sauf dispositions spécifiques prévues au sein du Formulaire d'abonnement, l'abonnement au Service ainsi qu'à ses éventuelles

options, est conclu pour une durée de douze (12) mois plus le mois en cours au jour de l'abonnement. En conséquence, tout abonnement aura pour échéance, le dernier jour du 13ème mois suivant celui de la réception par CGMF du formulaire d'abonnement dûment complété.

A l'issue de cette période, l'abonnement au Service et aux éventuelles options souscrites sera tacitement renouvelé par périodes de douze (12) mois, sauf résiliation du contrat à l'initiative de l'une des Parties, par lettre recommandée avec demande d'avis de réception adressée au moins trois (3) mois avant le terme de la période en cours.

Article 13 - Fin de contrat
Dans l'hypothèse d'une résiliation ou d'une fin de contrat, il est de la responsabilité du client de récupérer toutes ses données sauvegardées avant la date de fin du contrat via une restauration partielle ou complète.

CGMF s'engage à détruire à la date de fin de contrat + 10 jours, toutes les données sauvegardées en sa possession et à n'en conserver aucune copie, totale ou partielle.

Il s'assurera également qu'aucun des prestataires techniques externes ne conserve les dites Données.

Article 14 - Agrément Hébergement Données de Santé
La présence de données de santé à caractère personnel dans les données sauvegardées impose que le Service soit délivré dans les conditions réglementaires fixées par le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel. Ces dispositions ont pour objectif d'organiser et d'encadrer le dépôt, la conservation et la restitution des données de santé à caractère personnel, dans des conditions de nature à garantir leur confidentialité et leur sécurité.

Le Service est en cours d'agrément par le Ministre des Affaires sociales et de la Santé, ce qui garantira à terme une conformité totale de l'hébergement des données de santé à caractère personnel aux exigences légales et réglementaires. De plus amples informations sont disponibles à l'adresse Internet suivante :

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

Conformément aux dispositions du décret, l'hébergeur s'attache les services d'un médecin indépendant, aux termes d'un contrat, soumis au Conseil National de l'Ordre des Médecins.

Les principales missions du médecin de l'hébergeur sont les suivantes :
- ✓ Encadrement des procédures de restitution, de modification et de destructions de données ayant trait à la santé.
- ✓ Vérification de la cohérence d'informations (fiches santé, base de données, archives…), éventuellement suite à un incident.
- ✓ Vérification du respect déontologique en matière de données de santé à caractère personnel, pour l'ensemble du système.

Dans le cadre du Service, c'est le médecin de l'hébergeur qui est le seul habilité à pouvoir déchiffrer les données sauvegardées par le Client en cas de nécessité (ex. perte de la passphrase par le Client, demande d'un ayant droit…).

Nom et coordonnées du médecin de l'hébergeur :

M. Jean-Marc Lupoglazof
Hôpital Robert Debré, Unité de Cardiologie Néonatale
48, boulevard Sérurier
F-75019 Paris
Tel : 01 40 03 20 64
Fax : 01 40 03 24 70
E-mail : jean-marc.lupoglazof@rdb.ap-hop-paris.fr

Article 15 - Lieu d'hébergement
Conformément à l'article 68 de la loi Informatique et Libertés, le lieu d'hébergement des données doit se situer sur le territoire de l'Union Européenne (les pays membres ont mis en place un niveau de protection juridique et physique conforme aux exigences de la directive 95/46/CE relative à la protection des données personnelles).

Les centres d'hébergement de l'Hébergeur sont les suivants :
- ✓ Datacenters de CompuGroup Medical AG, situés à :
  - Maria Trost 21, D-56070 Coblence, Allemagne.
  - Via A. Olivetti 10, 70056 Molfetta (BA), Italie
- ✓ Datacenter du CAPITOLE/Level3 situé au 55, avenue des Champs Pierreux 92000 Nanterre, France.

Article 16 - Vos obligations concernant les Données à Caractère Personnel
En utilisant le Service, vous avez la possibilité de sauvegarder les données de santé et les données à caractère personnel de vos patients. Ces données sont notamment soumises à la protection conférée par les dispositions de la loi du 6 janvier 1978 dite « Informatique et Libertés ». En acceptant les présentes Conditions Générales d'Utilisation et Conditions Particulières, vous certifiez avoir valablement informé vos patients ou leurs représentants légaux pour l'ensemble des traitements de données que vous effectuez, en notamment le recours à un système de sauvegarde externalisé.

Par ailleurs, vous vous engagez à remplir l'ensemble des obligations découlant de la loi du 6 janvier 1978, et notamment celle d'informer les personnes concernées de leur droit d'accès, de modification et de suppression des données traitées.

Vous conservez à votre charge l'ensemble des déclarations, demandes d'autorisation et autres procédures et démarches à accomplir auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) afférentes aux traitements de données à caractère personnel que vous mettez en œuvre. Cette déclaration auprès de la CNIL doit se faire selon les modalités correspondant aux spécificités du traitement de ces données réalisé par le Client.

Nous tenons à vous rappeler qu'en tant que professionnel de la santé responsable de traitement de données à caractère personnel, vous avez des obligations particulières découlant de la loi du 6 janvier 1978 dite « Informatique et Libertés ». Pour plus d'informations sur vos obligations et les bonnes pratiques en matière de sécurité, nous vous invitons vivement à consulter le Guide de la CNIL adressé aux Professionnels de Santé en cliquant sur le lien hypertexte suivant :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_professionnels_de_sante.pdf

En tant que prestataire de santé, vous êtes soumis à des obligations professionnelles et déontologiques propre à votre métier. Nous vous rappelons que l'utilisation du Service s'effectue exclusivement sous votre responsabilité, notamment en ce qui concerne la protection des données des patients concernés. Nous déclinons toute responsabilité pour une éventuelle utilisation irrégulière des dites données.

Lors de votre première connexion au Service, il vous sera demandé de créer une passphrase afin de sauvegarder de manière chiffrée vos données externalisées. Cette passphrase étant strictement personnel et confidentiel, il vous est interdit de la communiquer à quiconque.

La robustesse de cette passphrase est assurée par une contrainte de saisie d'une longueur d'au minimum 8 caractères avec la présence obligatoire d'au moins une majuscule, une minuscule et un chiffre ou caractère spécial.

La même obligation vous incombe concernant les éléments personnels d'identification (identifiant et mot de passe) qui vous auront été transmis pour vous connecter au Service.

En cas de perte ou de vol de votre passphrase ou de vos éléments personnels d'identification, vous devez immédiatement en informer le centre de support CGMF aux coordonnées indiquées ci-dessous pour que nous puissions bloquer d'accès à vos sauvegardes.

Un service d'alerte par mail est également mis en place : celui-ci vous envoie un e-mail à chaque demande de restauration afin de vous permettre de détecter une éventuelle restauration illégitime de vos données réalisée à votre insu.

Nous vous rappelons par ailleurs que vous êtes responsable de votre poste de travail. Celui-ci doit être soumis à des mesures de sécurité particulières, afin notamment de répondre aux exigences de confidentialité. Nous vous conseillons :

- ✓ De protéger l'accès à votre poste informatique.
- ✓ D'utiliser un logiciel antivirus mis à jour régulièrement, ainsi qu'une application contre les logiciels espions (anti-spyware) et un « pare-feu » (firewall).
- ✓ De tenir à jour tous les logiciels et le système d'exploitation.
- ✓ De vérifier à chaque nouvelle connexion au Site Web du Service que l'indication de la date et l'heure de votre dernière connexion correspond à votre dernière visite.
- ✓ De contrôler la date et l'heure des restaurations effectuées, notamment grâce au service d'alerte par mail mis à disposition dans le cadre du Service.
- ✓ D'effacer les données présentes sur votre poste préalablement à sa réaffectation à une autre personne, à sa mise au rebut ou pour les postes partagés.

Article 17 – Notre responsabilité
Dans l'hypothèse d'un dysfonctionnement du Service, nous vous invitons à nous en informer immédiatement grâce à notre centre de support. Nous nous engageons au rétablissement des fonctions du Service dans les meilleurs délais.
Etant donné que l'Accès au Service s'effectue à distance, via le réseau Internet, il est soumis aux aléas techniques inhérents à l'Internet, et aux interruptions d'accès qui peuvent en résulter. De ce fait, nous ne pouvons pas être tenus responsables des difficultés d'accès ou impossibilité momentanée d'accès au Service dues à des perturbations des réseaux de télécommunication. En outre, l'accès au Service peut être momentanément interrompu pour des raisons de nécessité et notamment afin d'assurer la maintenance des serveurs.

En conséquence, notre responsabilité ne pourra être engagée de quelque manière que ce soit, et à quelque titre que ce soit, en cas notamment d'indisponibilité temporaire ou totale de tout ou partie du Service, d'une difficulté liée au temps de réponse, et d'une manière générale, d'un défaut de performance quelconque de tout ou partie du Service.

Nous ne vous offrons aucune garantie expresse ou tacite concernant notamment la capacité du Service à satisfaire vos besoins propres, l'absence d'erreur dans l'exploitation du Service, l'exactitude matérielle des données stockées par le Client sur nos serveurs.

Par ailleurs, sauf dispositions légales impératives contraires ou en cas de dommages corporels, d'atteinte à la vie ou à la santé d'autrui, nous ne pourrons en aucun cas être tenus responsables de tout dommage et/ou préjudice accessoire, incident ou indirect, de quelque nature que ce soit, notamment, et de manière non limitative, la perte de chiffre d'affaires, la perte de bénéfice, la perte d'une chance, la perte d'informations, l'atteinte à la vie privée, l'utilisation de données nominatives, et résultant de l'utilisation du Service, même si nous avons été avisés de l'éventualité de tels dommages.

Article 18 – Qualité, disponibilité et performance du service
Les données restaurées sont garanties d'être non-altérée et dans le même format qu'au moment de leurs sauvegardes.

Le service est disponible 24H/24H, 7J/7J. En cas de panne, la durée maximale d'interruption du service de restauration est de 4H. Si cette panne nécessite l'activation du plan de reprise d'activité (ex. destruction du site informatique principal), la durée maximale d'interruption du service de restauration est de 8H.
Selon la gravité de la panne, la durée d'interruption du service de sauvegarde peut atteindre une semaine.

Le centre de support est joignable au **0892 39 33 33** du lundi au vendredi de 9h à 18h sans interruption ou par mail à technique@lereseausantesocial.fr.

Le paramétrage du service permet une reprise automatique de la sauvegarde en cas de problème, jusqu'à la bonne exécution de celle-ci.
Les temps de réponse du service, que ce soit la durée d'exécution des sauvegardes/restaurations ou bien l'affichage des pages du portail Web sont fortement dépendant de la performance de l'accès Internet du Client (bande passante, temps de transit, erreurs…).
Afin de s'assurer de la qualité du Service, des indicateurs de performance et de disponibilité sont définis, analysés et réévalués par les équipes techniques CGMF.

Article 19 – Liste et rôles des prestataires techniques externes
CGMF a recours à des prestataires externes pour l'hébergement des infrastructures techniques dans des centres informatiques et le raccordement à Internet.

CGMF se porte garant du respect par ces prestataires des obligations leur incombant aux termes du Contrat, en particulier des exigences de confidentialité et de disponibilité.

La liste de ces prestataires est disponible sur simple demande via le service de support.

Article 20 – Suspension du droit d'accès
Dans l'hypothèse d'un non-respect d'une quelconque de vos obligations prévues dans les présentes Conditions Particulières, nous nous réservons le droit de suspendre sans préavis votre accès au Service, sans préjudice d'éventuelles demandes d'indemnisation de notre part. Nous vous informerons de la suspension de votre accès et des raisons de celle-ci par courrier électronique et vous inviterons à nous contacter sans délai, afin de tenter de résoudre les problèmes éventuels.

Durant cette suspension, les données déjà sauvegardées restent stockées sur les infrastructures informatiques de CGMF mais le Client n'a plus la possibilité d'y stocker de nouvelles sauvegardes.

Article 21 – Défaillance de l'hébergeur
En cas de défaillance de CGMF (liquidation judiciaire, perte de l'agrément d'hébergeur ou impossibilité d'exercer l'activité d'hébergement…), ce dernier s'engage à tout mettre en œuvre pour assurer la continuité ou le transfert d'activité vers un autre prestataire.

Le Client pourra en outre récupérer ses Données selon les modalités décrites à l'article 13.