(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
24 décembre 2003 (24.12.2003)

PCT

(10) Numéro de publication internationale
WO 03/107150 A1

(51) Classification internationale des brevets[7] : G06F 1/00, 19/00

(21) Numéro de la demande internationale : PCT/FR03/01665

(22) Date de dépôt international : 3 juin 2003 (03.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/07499 18 juin 2002 (18.06.2002) FR

(71) Déposant : PATIENT ON LINE [FR/FR]; 171 avenue Ledru-Rollin, F-75011 PARIS (FR).

(71) Déposants et
(72) Inventeurs : VADROT, Dominique [FR/FR]; 16, rue Maurice Berthelemy, F-94120 FONTENAY SOUS BOIS (FR). VERDOUX, Martine [FR/FR]; 65, rue Nicolo, F-75116 PARIS (FR).

(74) Mandataires : BLOT, Philippe etc.; 2, place d'Estienne d'Orves, F-75441 PARIS CEDEX 09 (FR).

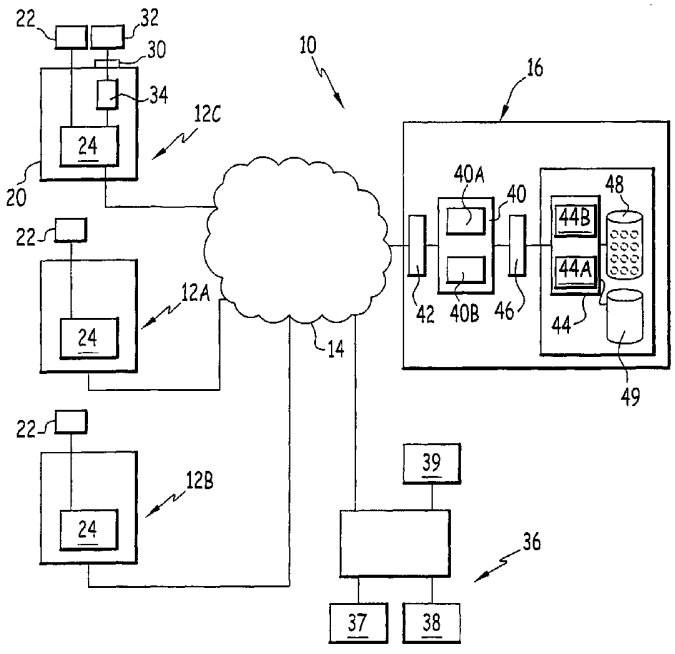
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[Suite sur la page suivante]

(54) Title: DATA MANAGEMENT SYSTEM FOR EMERGENCY SITUATION

(54) Titre : SYSTEME DE GESTION D'INFORMATIONS POUR SITUATION D'URGENCE



(57) Abstract: The invention concerns a system comprising: at least one database (48) for storing said data, one identifier of the first entity concerned by each data; and at least one querying station (36) including means for accessing the databases (48); means for defining warning data among the data; means (49) for associating an emergency access code with the warning data. The access means include means for inputting the emergency access code and means for providing the warning data concerning a first entity without providing the identifier of the first entity.

[Suite sur la page suivante]

WO 03/107150 A1

TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Ce système comprend :- au moins une base de données (48) pour le stockage : desdites informations ; d'un identifiant de la première entité concernée par chaque in-formation ; et- au moins un poste d'interrogation (36) comprenant des moyens d'accès à; la base de données (48),- des moyens pour définir des informations d'alerte parmi les informations ; - des moyens (49) pour associer un code d'accès d'urgence aux informations d'alerte.Les moyens d'accès comportent des moyens d'entrée du code d'accès d'urgence et des moyens pour mettre à disposition les informations d'alerte concernant une première entité sans que l'identifiant de la première entité ne soit mis à disposition.

Système de gestion d'informations pour situation d'urgence

La présente invention concerne un système de gestion d'informations, et notamment d'informations médicales, chaque information concernant une première entité, le système comprenant :

- au moins une base de données pour le stockage :
  - desdites informations ;
  - d'un identifiant de la première entité concernée par chaque information, chaque information étant associée à l'identifiant de la première entité concernée ; et
- au moins un poste d'interrogation comprenant des moyens d'accès à la ou chaque base de données pour la consultation desdites informations.

Dans de nombreux domaines, il est nécessaire de pouvoir assurer le stockage confidentiel et la consultation autorisée et contrôlée d'informations validées concernant une personne.

Ces informations peuvent être par exemple des informations médicales concernant un patient. Ces informations médicales sont engendrées par un ou plusieurs praticiens médicaux soumis à des obligations déontologiques. En particulier, ces obligations déontologiques imposent aux praticiens le respect du secret professionnel, de sorte qu'il est interdit aux praticiens de rendre accessibles ces informations sans l'autorisation du patient concerné et le patient doit pouvoir accéder aux informations le concernant.

Les obligations déontologiques des praticiens rendent difficiles l'exploitation des données concernant le patient en cas d'urgence. En particulier, si le patient est victime d'un malaise sur le voie publique, les services d'urgence prenant en charge le patient ne peuvent accéder directement aux informations médicales concernant le patient, dans la mesure où ce service d'urgence n'a pas été préalablement autorisé à accéder à ces informations et que le patient n'est pas nécessairement facilement identifiable notamment s'il est inconscient.

L'invention a pour but un système de gestion d'informations permettant de rendre accessible des informations utiles, même lorsque la personne concernée par ses informations n'est pas consciente, tout en garantissant le respect des obligations déontologiques.

A cet effet, l'invention a pour objet un système de gestion d'informations du type précité, caractérisé en ce qu'il comporte :

- des moyens pour définir des informations d'alerte parmi lesdites informations ;
- des moyens pour associer un code d'accès d'urgence, aux informations d'alerte concernant une même première entité, le code d'accès d'urgence étant différent de l'identifiant de la première entité; et

en ce que lesdits moyens d'accès comportent des moyens d'entrée du code d'accès d'urgence et des moyens pour, lors de l'entrée du code d'accès d'urgence associé à l'identifiant d'une première entité, mettre à disposition les informations d'alerte concernant la première entité associée au code d'accès d'urgence, sans que l'identifiant de la première entité ne soit mis à disposition.

Suivant des modes particuliers de réalisation, le système de gestion d'informations comporte l'une ou plusieurs des caractéristiques suivantes :

- il comprend :
  - des moyens pour créer au moins un évènement regroupant, de manière indissociable, dans une même donnée élémentaire :
    - la ou chaque information concernant la première entité ; et
    - l'identifiant de la première entité ; et
  - des moyens de stockage définitif du contenu du ou de chaque évènement, chacun en tant que donnée élémentaire dans la ou chaque base de données ;
- les moyens pour définir des informations d'alerte parmi les informations comportent :
  - des moyens pour fixer, pour chaque information, un indicateur d'alerte représentatif de la définition des informations ;
  - des moyens pour intégrer dans la donnée élémentaire correspondant à l'évènement contenant ladite information, l'indicateur d'alerte représentatif de la définition des informations ; et

- des moyens pour intégrer dans la donnée élémentaire correspondant à l'évènement contenant ladite information, l'indicateur d'alerte,

et lesdits moyens pour mettre à disposition les informations d'alerte comportent des moyens d'analyse de l'indicateur d'alerte contenu dans chaque évènement contenant l'identifiant de la première entité associée au code d'accès d'urgence, et les moyens pour mettre à disposition les informations d'alerte sont adaptés pour mettre à disposition la ou chaque information contenue dans l'évènement, si l'analyse de l'indicateur d'alerte montre que la ou chaque information est une information d'alerte ;

- le système comporte des moyens pour intégrer dans chaque donnée élémentaire correspondant à un évènement un identifiant d'une seconde entité ayant engendrée ladite information ;

- lesdits moyens pour associer un code d'accès d'urgence, aux informations d'alerte concernant une même première entité comportant une base de données établissant une correspondance entre chaque code d'accès d'urgence et un identifiant d'une première entité ; et

- le système comporte des moyens de génération aléatoire d'un code d'accès d'urgence pour chaque nouvel identifiant d'une première entité.

L'invention a également pour objet un procédé de gestions d'informations, chaque information concernant une première entité dans un système comprenant :

- au moins une base de données pour le stockage :
  - desdites informations ;
  - d'un identifiant de la première entité concernée par chaque information, chaque information étant associée à l'identifiant de la première entité ;
- au moins un poste d'interrogation comprenant des moyens d'accès à la ou chaque base de données pour la consultation desdites informations, et
- des moyens pour définir des informations d'alerte parmi lesdites informations, et

dans lequel un code d'accès d'urgence est associé aux informations d'alerte concernant une même première entité, le code d'accès d'urgence étant différent de l'identifiant de la première entité,

caractérisé en ce qu'il comprend l'entrée depuis lesdits moyens d'accès, d'un code d'accès d'urgence, et, lors de l'entrée dudit code d'accès d'urgence associé à l'identifiant d'une première entité, la mise à disposition des informations d'alerte concernant la première entité associée au code d'accès d'urgence, sans que l'identifiant de la première entité ne soit mis à disposition.

L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins, sur lesquels :

- la figure 1 est une vue schématique d'un système de gestion d'informations selon l'invention ;
- la figure 2 est une vue schématique illustrant le format d'une donnée élémentaire utilisée par le système de gestion d'informations de la figure 1 ;
- la figure 3 est un organigramme de l'algorithme principal mis en œuvre dans le système, et
- la figure 4 est un organigramme de l'algorithme de consultation d'urgence du système selon l'invention.

Le système de gestion d'informations 10 selon l'invention est illustré schématiquement sur la figure 1. Celui-ci comporte, d'une part, un ensemble de postes utilisateurs désignés par la référence générale 12, chacun relié à un réseau 14 collectif de transmission d'informations tel que le réseau Internet et, d'autre part, un centre 16 de stockage et de gestion des informations.

Le système de gestion d'informations 10 est destiné, dans l'exemple considéré, à la gestion d'informations médicales concernant des patients identifiés. Ces informations sont engendrées par des praticiens médicaux tels que des médecins, des radiologues ou des biologistes en charge d'un laboratoire d'analyses.

En particulier, le système de gestion est adapté pour permettre le stockage définitif d'une information dans le centre 16 de stockage, sans que cette information ne puisse être ultérieurement modifiée. De plus, il est

conservé, associés à cette information, au moins un identifiant du patient concerné, ainsi qu'un identifiant du praticien ayant engendré l'information.

Le système permet de donner accès à une information stockée à partir de l'identifiant du patient seulement au patient concerné et au praticien ayant engendré l'information, ainsi que, éventuellement, après accord du patient, à d'autres praticiens.

En outre, le système permet l'accès à certaines informations stockées concernant un patient par des personnes disposant d'un code d'accès d'urgence. Les informations sont alors mises à disposition en nombre réduit, et sans que l'identifiant du patient concerné par ces informations ne soit mis à disposition.

Chaque entité intervenant dans le système, qu'il s'agisse d'un patient ou d'un praticien, est équipé ou a accès à un poste d'utilisateur 12. Ainsi, par exemple, un premier poste d'utilisateur 12A équipe le cabinet d'un médecin généraliste et un poste d'utilisateur 12B équipe le domicile d'un patient. De même, par exemple, un laboratoire d'imageries médicales est équipé d'un poste d'utilisateur 12C.

Chaque poste d'utilisateur 12A, 12B, 12C comporte un micro-ordinateur 20 équipé d'un navigateur Internet adapté. Il est relié par une interface adaptée au réseau 14. Chaque poste d'utilisateur comporte des moyens 22 de recueil de données d'entrée tels qu'un clavier ou un module de conversion de données. A partir du clavier, peuvent être entrés notamment une information médicale, un identifiant d'un patient tel que son nom, ainsi qu'un identifiant du praticien ayant produit l'information.

Chaque poste d'utilisateur 12 est adapté pour mettre en œuvre, depuis des moyens de traitement d'informations 24, des moyens logiciels d'accès au centre 16 de stockage et de gestion des informations.

Selon l'invention, chaque poste d'utilisateur 12A, 12B, 12C comporte des moyens logiciels pour créer un évènement regroupant de manière indissociable dans une même donnée élémentaire, des informations recueillies concernant un patient, un identifiant du patient et un identifiant du praticien. Ces moyens de création d'un évènement sont avantageusement téléchargés depuis le centre 16 et sont par exemple constitués d'une page

depuis le centre 16 et sont par exemple constitués d'une page au format HTML (Hyper Text Markup Language) formant interface de dialogue.

Certains de ces postes d'utilisateur, comme le poste 12C, comportent, en plus du micro-ordinateur 20, une interface 30 de connexion du micro-ordinateur à une installation 32 d'imagerie médicale ou de recueil d'informations médicales apte à produire des images ou informations numériques sous un format prédéfini tel que le format DICOM Hprim HL7. Par nature, cette image ou information numérique comporte un identifiant du patient concerné. Le poste d'utilisateur met en œuvre en outre un module logiciel 34 propre à analyser l'image numérique produite par l'installation 32 et à extraire de celle-ci un identifiant du patient concerné.

En outre, le système comporte des postes d'interrogation 36 reliés au centre 16 de stockage et de gestion des informations au travers du réseau 14. Chaque poste d'interrogation 36 est constitué par n'importe quel micro-ordinateur 20 équipé d'un navigateur internet adapté. Ces postes d'interrogation n'ont pas à être identifiés initialement par le centre de stockage et de gestion des informations 16.

Chaque poste d'interrogation 36 comporte des moyens d'entrée d'un code d'accès d'urgence, tels qu'un clavier 37, ou un lecteur de carte à puce 38 ainsi qu'un périphérique de mise à disposition d'informations tel qu'un écran ou une imprimante 39.

Le centre de stockage et de gestion des informations 16 comporte un ensemble de serveurs 40 pour la gestion des accès au centre 16. Cet ensemble de serveurs 40 comporte notamment un serveur d'authentification 40A adapté, comme connu en soi, pour identifier l'origine d'une requête adressée au centre serveur. Il comporte en outre un ou plusieurs serveurs 40B propres à la gestion d'échange de fichiers exécutables et de pages HTML suivant le protocole HTTP entre le centre de stockage et de gestion 16 et les postes d'utilisateurs. En particulier, le ou chaque serveur 40B comporte un module logiciel propre à assurer le téléchargement dans chaque poste utilisateur demandeur de pages HTML constituant des interfaces utilisateurs permettant l'accès aux informations stockées, ainsi que la sauvegarde de nouvelles informations. Cet ensemble de serveurs 40 est relié di-

rectement au réseau 14 au travers d'une première barrière de sécurité 42 (firewalls).

L'ensemble des serveurs de gestion d'accès 40 est relié en outre à un ensemble de serveurs 44 de gestion d'évènements au travers d'une seconde barrière de sécurité 46 (firewalls). En particulier, l'ensemble de serveurs 44 est propre à mettre en œuvre un module logiciel 44A de transcription des images numériques reçues dans des formats différents notamment au format DICOM en un même format, par exemple le format XML.

L'ensemble de serveurs 44 est propre en outre à mettre en œuvre un module logiciel 44B de gestion du stockage d'évènements dans une unité de stockage 48 et de gestion des accès à ces évènements.

Cette unité de stockage 48 est destinée à la mémorisation permanente d'une ou plusieurs bases de données dont les données élémentaires sont constituées par des évènements définis par les postes utilisateurs et comportant notamment les informations à sauvegarder.

En outre, une unité supplémentaire 49 de stockage est reliée à l'ensemble de serveurs 44. Cette unité de stockage est destinée à la mémorisation permanente d'une base de données dans laquelle est stocké, pour chaque identifiant d'un patient concerné par des informations, un code d'accès d'urgence associé.

Le code d'accès d'urgence est défini aléatoirement par le module de gestion 44B pour chaque nouveau patient géré par le système. Le code est différent de l'identifiant du patient tel que son nom.

Le code d'accès d'urgence est inscrit sur une carte remise au patient. Sur cette carte figure également l'adresse IP du centre 16 de stockage et de gestion des informations.

En variante, le code d'accès d'urgence est mémorisé dans une carte à mémoire pouvant être lu dans un lecteur de carte d'un ordinateur. Cette carte porte également l'adresse IP du centre 16.

Sur la figure 2 est représentée schématiquement la structure d'une donnée élémentaire stockée dans la base de données 48. Celle-ci correspond à un évènement.

Chaque évènement comporte au moins une information proprement dite 52. Cette information est constituée par exemple de données numériques correspondant au résultat d'une analyse ou d'un texte correspondant à l'avis d'un praticien sur l'état clinique d'un patient. Une information peut également être constituée par un fichier rattaché à l'évènement tel qu'un document au format HTML ou un fichier image au format DIBCOM ou une pièce jointe dans un format bureautique.

En outre, chaque évènement comporte un identifiant 54 d'une première entité. Cet identifiant désigne le patient concerné par les informations 52. De même, l'évènement comporte un identifiant 56 d'une seconde entité. Cet identifiant désigne le praticien ayant produit l'information.

Avantageusement, chaque évènement comporte une liste 58 des identifiants d'entités supplémentaires pouvant avoir accès aux informations.

L'évènement comporte également avantageusement mais non obligatoirement d'autres informations à remplir par l'utilisateur telles que :

- un titre ;
- une date de création et/ou de compléments de l'évènement ; et
- une liste de mots clés.

En outre, chaque évènement comporte un indicateur d'alerte constitué d'un indicateur bouléen indiquant dans son premier état (valide) que les informations contenues dans l'évènement constituent des informations d'alerte pouvant être communiquées en cas d'urgence, et dans son deuxième état (non valide), que les informations contenues dans l'évènement ne doivent pas être communiquées en cas d'urgence.

Pour l'ajout d'une information dans le centre de stockage, le complément d'une information pré-existante par une information supplémentaire, la modification des droits d'accès à une information, la modification de l'indicateur d'alerte d'une information ou la consultation d'une information, l'utilisateur se connecte depuis un poste d'utilisateur 12 au centre de stockage 16.

L'algorithme de la figure 3 est alors mis en œuvre.

Le poste d'utilisateur 12 peut être constitué, pour les opérations les plus simples, seulement d'un micro-ordinateur relié au réseau Internet à

l'aide d'un navigateur de tout type adapté. Après connexion du poste d'utilisateur, à l'étape 100, l'ensemble de serveurs 40 du centre de stockage 16 retourne une interface de dialogue au format HTML au poste d'utilisateur 12, à l'étape 102. A l'étape 104, le centre 16 procède au travers de l'interface de dialogue mise en œuvre par le poste d'utilisateur à une authentification de l'utilisateur. En fonction de l'identifiant entré par l'utilisateur, des contrôles des actions autorisées à celui-ci sont effectués, à l'étape 106, et un contrôle des droits d'accès de l'utilisateur est réalisé, à l'étape 108.

L'utilisateur est alors libre de procéder à plusieurs opérations en fonction des actions qui lui sont autorisées. Il procède, à partir de l'interface mise à sa disposition, à l'étape 110, au choix d'une opération à réaliser.

Celle-ci peut être l'entrée d'une information nouvelle dans le centre de stockage 16. La branche 110A de l'organigramme est alors mise en œuvre.

Il peut s'agir également de l'ajout d'une information supplémentaire pour compléter une information déjà présente dans le centre de stockage 16. La branche 110B de l'organigramme est alors mise en œuvre.

L'utilisateur praticien peut également modifier les droits d'accès aux informations stockées en habilitant un nouveau praticien à accéder aux informations concernant un patient. La branche 110C de l'organigramme est alors mise en œuvre.

Lorsque le praticien souhaite modifier l'indicateur d'alerte d'un évènement, la branche 110D de l'algorithme est mise en œuvre.

L'utilisateur peut également prendre seulement connaissance d'informations stockées dans le centre de stockage par mise en œuvre de la branche 110E de l'organigramme.

Lorsque un praticien souhaite entrer une nouvelle information dans le centre 16, l'algorithme diffère suivant que l'information médicale que souhaite entrer le praticien peut être associée automatiquement à un patient constituant une première entité, ou que la liaison au patient doit être réalisée manuellement. Ce choix est effectué à l'étape 111.

Si l'information ne contient pas initialement l'identifiant du patient concerné, l'information est entrée par le praticien, par exemple au clavier, à l'étape 112. Une identification du patient concerné est saisie, à l'étape 114,

notamment par sélection d'un identifiant du patient parmi une liste d'identifiants de patients ou par frappe au clavier.

En revanche, et dans le cas d'un poste d'utilisateur tel que le poste 12C, la reconnaissance de l'identifiant du patient concerné peut se faire automatiquement lors de l'entrée de l'information. Ainsi, l'information contenant l'identifiant du patient concerné est entrée, à l'étape 122, par exemple au travers de l'interface 30. Cette information est par exemple constituée d'une image médicale au format DICOM. A l'étape 124, le module logiciel 36 procède à une analyse de l'image et à une reconnaissance de l'identifiant du patient dans l'image transmise.

A l'étape 130, le praticien définit la liste des identifiants des entités supplémentaires autorisées à accéder aux informations contenues dans l'évènement. Cette étape consiste à définir la liste 58 des identifiants des praticiens autorisés à accéder.

A l'étape 131, le praticien définit l'indicateur d'alerte en précisant si l'information contenue dans l'évènement peut ou non être rendue accessible en cas d'urgence suivant une procédure décrite dans la suite de la description.

Si le praticien souhaite rendre cette information accessible en cas d'urgence, il s'assure que l'information en elle-même ne contient pas de données permettant d'identifier le patient comme son nom.

A l'étape 132, le praticien valide, par saisie d'un code de signature, l'ensemble des éléments constituant l'évènement, à savoir l'information médicale proprement dite, l'identifiant du patient concerné, son propre identifiant,la liste des identifiants des entités supplémentaires autorisées à accéder, et l'indicateur d'alerte. A l'issue de cette étape, les éléments constituant l'évènement ne peuvent plus être modifiés et l'évènement peut seulement être complété.

A l'étape 134, le poste d'utilisateur 12 assure la création d'une donnée élémentaire reprenant les différents éléments de l'évènement. Cette donnée élémentaire est cryptée par tout procédé adapté et est adressée par l'interface de dialogue au centre 16 de stockage et de gestion des informations.

A sa réception, la donnée élémentaire est traitée par les serveurs de gestion d'évènements 44, à l'étape 136. Si la donnée élémentaire contient des images numériques dans des formats différents du format XML, ces images sont automatiquement converties au format XML, à l'étape 138, et la donnée élémentaire est complétée par des données images au format XML en plus des données images dans un autre format.

La donnée élémentaire ainsi retraitée est sauvegardée définitivement dans l'unité de stockage 48, à l'étape 140.

Lorsque l'utilisateur souhaite compléter un évènement en ajoutant une information supplémentaire, les étapes de la branche 110B sont mises en œuvre après l'étape 110.

A l'étape 150, l'évènement à compléter est sélectionné.

La donnée élémentaire correspondant à l'évènement sélectionné est transmise par le centre 16 au poste utilisateur, à l'étape 152. La donnée élémentaire n'est transmise que si l'identifiant de l'utilisateur est compris dans l'évènement en cause, soit qu'il s'agisse du patient concerné, du praticien à l'origine de l'information ou d'un praticien supplémentaire dont l'identifiant figure dans la liste 58.

L'information supplémentaire est entrée à l'étape 154, soit manuellement depuis le clavier, soit par reprise d'un fichier déjà existant. Dans ce dernier cas, l'information supplémentaire constitue un nouveau fichier attaché.

A l'étape 156, l'utilisateur valide l'ajout de l'information par entrée d'un code de signature.

L'information supplémentaire est ajoutée à l'étape 158 pour former une nouvelle donnée élémentaire constituant l'évènement modifié. En outre, la date, et l'identifiant de l'utilisateur ayant ajouté l'information, ainsi qu'un lien avec l'information sont ajoutés dans la donnée élémentaire pour assurer un suivi des modifications. La nouvelle donnée élémentaire ainsi constituée est ensuite traitée conformément aux étapes 136 et suivantes.

Lorsque l'utilisateur souhaite modifier un droit d'accès, celui-ci peut seulement ajouter de nouveaux identifiants d'utilisateur habilités à accéder à une information donnée. A cet effet, l'évènement dont les accès sont à com-

pléter est sélectionné à l'étape 200. La donnée élémentaire correspondant à l'évènement sélectionné est alors transmise au poste utilisateur à l'étape 202. La donnée élémentaire n'est transmise que si l'identifiant de l'utilisateur est compris dans l'évènement en cause, soit qu'il s'agisse du patient concerné, du praticien à l'origine de l'information ou d'un praticien supplémentaire dont l'identifiant figure dans la liste 58.

A l'étape 204, l'utilisateur sélectionne ou entre au clavier un ou plusieurs identifiants supplémentaires d'utilisateurs habilités à accéder à l'information puis il valide, à l'étape 206, les nouveaux identifiants. Les identifiants supplémentaires sont ajoutés dans la donnée élémentaire constituant l'évènement à l'étape 208. En outre, la date, et l'identifiant de l'utilisateur ayant ajouté les nouveaux identifiants, ainsi qu'un lien avec les nouveaux identifiants sont ajoutés dans la donnée élémentaire pour assurer un suivi des modifications. Les étapes 136 et suivantes sont alors à nouveau mises en œuvre.

Lorsque l'utilisateur, et notamment le praticien souhaite modifier l'indicateur d'alerte associé à une information, afin de rendre accessible cette information en cas d'urgence, ou au contraire ne pas mettre à disposition cette information, la branche 110D de l'algorithme est mise en œuvre.

A l'étape 210 l'évènement dont l'indicateur d'alerte doit être modifié est sélectionné. La donnée élémentaire correspondant à l'évènement sélectionné est transmise au poste utilisateur 12 à l'étape 212, sous réserve que l'identifiant de l'utilisateur soit compris dans l'évènement en cause parce qu'il s'agit du patient concerné, du praticien à l'origine de l'information ou d'un praticien supplémentaire dont l'identificateur figure dans la liste 58.

A l'étape 214, l'utilisateur change l'état de l'indicateur d'alerte, par exemple par validation à l'écran d'une zone prédéfinie. Si le praticien souhaite rendre cette information accessible en cas d'urgence, il s'assure que l'information en elle-même ne contient pas de données permettant d'identifier le patient comme son nom. L'évènement modifié est alors validé ensuite à l'étape 216.

La nouvelle valeur de l'indicateur d'alerte est ajoutée dans la donnée élémentaire constituant l'évènement à l'étape 218.

En outre, la date et l'identifiant de l'utilisateur ayant modifié l'indicateur d'alerte sont ajoutés dans la donnée élémentaire pour assurer un suivi des modifications.

Les étapes 136 et suivantes sont alors à nouveau mises en œuvre.

Pour la consultation des informations stockées dans le centre 16, et depuis n'importe quel poste d'utilisateur 12, les étapes de la branche 110E sont mises en œuvre.

A l'étape 250, une requête est formulée par l'utilisateur depuis le poste d'utilisateur. Celle-ci est prise en compte par les serveurs de gestion des évènements 44, à l'étape 252. En fonction des droits d'accès contenus dans l'évènement en cause dans la requête, et en fonction des droits de l'utilisateur, le contenu de la donnée élémentaire est transmis du centre de stockage 16 au poste utilisateur 12, à l'étape 254.

En particulier, la donnée élémentaire n'est transmise que si l'identifiant de l'utilisateur est compris dans l'évènement en cause dans la requête, soit qu'il s'agisse du patient concerné, du praticien à l'origine de l'information ou d'un praticien supplémentaire dont l'identifiant figure dans la liste 58.

L'information est alors mise à disposition de l'utilisateur à l'étape 256, par exemple par affichage, ou bien par sauvegarde du contenu de la donnée élémentaire sur le disque dur du poste utilisateur.

A l'étape 258, un journal des accès est mis à jour dans le centre 16 pour enregistrer l'identifiant de l'utilisateur, la nature de l'information mise à disposition, la date d'accès fournie par le système et toute autre information utile.

Afin de permettre que des informations nécessaires en cas d'urgence puissent être rendues accessibles aux services de secours, que ceux-ci soient des praticiens de santé ou non, le patient, dont les informations sont stockées dans le système, porte sur lui la carte sur laquelle figure l'adresse IP du centre 16 de gestion et de stockage d'informations sur le réseau 14, ainsi que le code d'accès d'urgence associé au patient.

Pour permettre l'accès aux informations d'alerte, l'algorithme de la figure 4 est mise en œuvre.

Lorsque le patient nécessite des soins médicaux, alors que celui-ci n'est pas chez un praticien habilité à accéder aux informations, le patient peut fournir à n'importe quel interlocuteur la carte qu'il porte sur lui pour permettre à son interlocuteur d'accéder à certaines informations d'alerte que le patient a préalablement sélectionnées en plaçant ou faisant placer les indicateurs d'alerte associés à ces informations dans un état valide prédéterminé.

Au cas où le patient est inanimé, les services de secours peuvent se saisir de la carte portée par le patient et effectuer eux-mêmes le recueil des informations d'urgence.

A cet effet, à l'étape 402, le service de secours se connecte au centre 16 de stockage et de gestion des informations grâce à l'adresse IP mentionnée sur la carte portée par le patient. Cette connexion peut être effectuée depuis n'importe quel ordinateur connecté au réseau 14 et disposant d'un navigateur internet adapté. Cet ordinateur forme alors un poste d'interrogation 36.

Après connexion, le centre 16 assure à l'étape 404 le chargement dans le poste d'interrogation 36 d'une interface d'utilisateur. A l'étape 406, le service de secours est invité à entrer le code d'accès d'urgence propre au patient. Ce code d'accès d'urgence étant totalement indépendant de l'identifiant du patient, l'identifiant du patient n'est pas nécessaire pour l'entrée du code d'alerte.

Le module logiciel 44B de gestion des accès aux évènements stockés détermine à l'étape 408 si le code d'accès d'urgence est ou non associé à un identifiant connu, par interrogation de la base de données hébergée dans l'unité de stockage 49.

Si le code d'accès d'alerte est inconnu, l'étape 406 est à nouveau mise en œuvre.

En revanche, si le code d'accès d'alerte est connu, le centre 16 de stockage et de gestion des informations détermine à l'étape 410 l'identifiant du patient concerné.

A l'étape 412, le module logiciel 44B de gestion des évènements recherche, parmi les évènements stockés, les évènements contenant

l'identifiant de la première entité. Parmi ces évènements trouvés, il analyse à l'étape 414 l'indicateur d'alerte associé à chaque évènement. Il sélectionne parmi les évènements ceux dont les indicateurs d'alerte sont dans un état valide indiquant que les informations contenues dans l'évènement peuvent être communiquées en cas d'urgence.

A l'étape 416, le centre 16 assure la transmission, sans cryptage des informations contenues dans chacun des seuls évènements de la base 48 dont l'indicateur d'alerte est valide, et dont l'identifiant de la première entité est l'identifiant associé au code d'accès d'alerte dans la base 49.

Les informations transmises sont communiquées sans que l'identifiant de la première entité ne soit transmis.

A l'étape 418, les informations transmises sont mises à disposition du service d'urgence, par exemple par affichage de ces informations sur l'écran du poste d'interrogation 36.

A l'étape 420, le journal des accès est mis à jour dans le centre 16 par enregistrement de la nature de l'information mise à disposition, la date d'accès fournie par le système ou toute autre information utile.

On conçoit qu'avec un tel système de gestion d'informations, des informations utiles au traitement du patient en cas d'urgence peuvent être mises à disposition à tout service de secours, sans que l'identité du patient ne soit dévoilée, et en permettant que seules les informations nécessaires préalablement sélectionnées avec l'accord du patient soit transmise au service de secours lors de son intervention.

En outre, l'accès à ces informations est très simple et est rendue possible même si le service de secours n'est pas normalement habilité à intervenir sur le système et même si le patient est inconscient.

REVENDICATIONS

1.- Système de gestion d'informations, chaque information concernant une première entité, le système comprenant :

- au moins une base de données (48) pour le stockage :
  - desdites informations (52) ;
  - d'un identifiant de la première entité concernée par chaque information, chaque information étant associée à l'identifiant de la première entité concernée ; et
- au moins un poste d'interrogation (36) comprenant des moyens d'accès à la ou chaque base de données (48) pour la consultation desdites informations,

caractérisé en ce qu'il comporte :

- des moyens pour définir des informations d'alerte parmi lesdites informations ;
- des moyens (49) pour associer un code d'accès d'urgence, aux informations d'alerte concernant une même première entité, le code d'accès d'urgence étant différent de l'identifiant de la première entité; et

en ce que lesdits moyens d'accès comportent des moyens d'entrée du code d'accès d'urgence et des moyens pour, lors de l'entrée du code d'accès d'urgence associé à l'identifiant d'une première entité, mettre à disposition les informations d'alerte concernant la première entité associée au code d'accès d'urgence, sans que l'identifiant de la première entité ne soit mis à disposition.

2. Système de gestion d'informations selon la revendication 1, caractérisé en ce qu'il comprend :

- des moyens (12) pour créer au moins un évènement regroupant, de manière indissociable, dans une même donnée élémentaire (50) :
  - la ou chaque information (52) concernant la première entité ; et
  - l'identifiant (54) de la première entité ; et
- des moyens (12, 44, 48) de stockage définitif du contenu du ou de chaque évènement, chacun en tant que donnée élémentaire (50) dans la ou chaque base de données (48).

3. Système de gestion d'informations, caractérisé en ce que les moyens (12) pour définir des informations d'alerte parmi les informations comportent :

- des moyens pour fixer, pour chaque information, un indicateur d'alerte (59) représentatif de la définition des informations ;

- des moyens pour intégrer dans la donnée élémentaire correspondant à l'évènement contenant ladite information, l'indicateur d'alerte (59) représentatif de la définition des informations ; et

- des moyens pour intégrer dans la donnée élémentaire correspondant à l'évènement contenant ladite information, l'indicateur d'alerte (59),

et en ce que lesdits moyens pour mettre à disposition les informations d'alerte comportent des moyens d'analyse de l'indicateur d'alerte (59) contenu dans chaque évènement contenant l'identifiant de la première entité associée au code d'accès d'urgence, et les moyens pour mettre à disposition les informations d'alerte sont adaptés pour mettre à disposition la ou chaque information contenue dans l'évènement, si l'analyse de l'indicateur d'alerte montre que la ou chaque information est une information d'alerte.

4. Système de gestion d'informations selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens pour intégrer dans chaque donnée élémentaire correspondant à un évènement un identifiant d'une seconde entité ayant engendrée ladite information.

5. Système de gestion d'informations selon l'une quelconque des revendications, caractérisé en ce que lesdits moyens pour associer un code d'accès d'urgence, aux informations d'alerte concernant une même première entité comportant une base de données (49) établissant une correspondance entre chaque code d'accès d'urgence et un identifiant d'une première entité.

6. Système de gestion d'informations selon l'une quelconque des revendications, caractérisé en qu'il comporte des moyens de génération aléatoire d'un code d'accès d'urgence pour chaque nouvel identifiant d'une première entité.

7. Procédé de gestion d'informations, chaque information concernant une première entité dans un système comprenant :

- au moins une base de données (48) pour le stockage :
  - desdites informations (52) ;
  - d'un identifiant de la première entité concernée par chaque information, chaque information étant associée à l'identifiant de la première entité ;

- au moins un poste d'interrogation (36) comprenant des moyens d'accès à la ou chaque base de données (48) pour la consultation desdites informations, et

- des moyens pour définir des informations d'alerte parmi lesdites informations, et

dans lequel un code d'accès d'urgence est associé aux informations d'alerte concernant une même première entité, le code d'accès d'urgence étant différent de l'identifiant de la première entité,

caractérisé en ce qu'il comprend l'entrée depuis lesdits moyens d'accès, d'un code d'accès d'urgence, et, lors de l'entrée dudit code d'accès d'urgence associé à l'identifiant d'une première entité, la mise à disposition des informations d'alerte concernant la première entité associée au code d'accès d'urgence, sans que l'identifiant de la première entité ne soit mis à disposition.

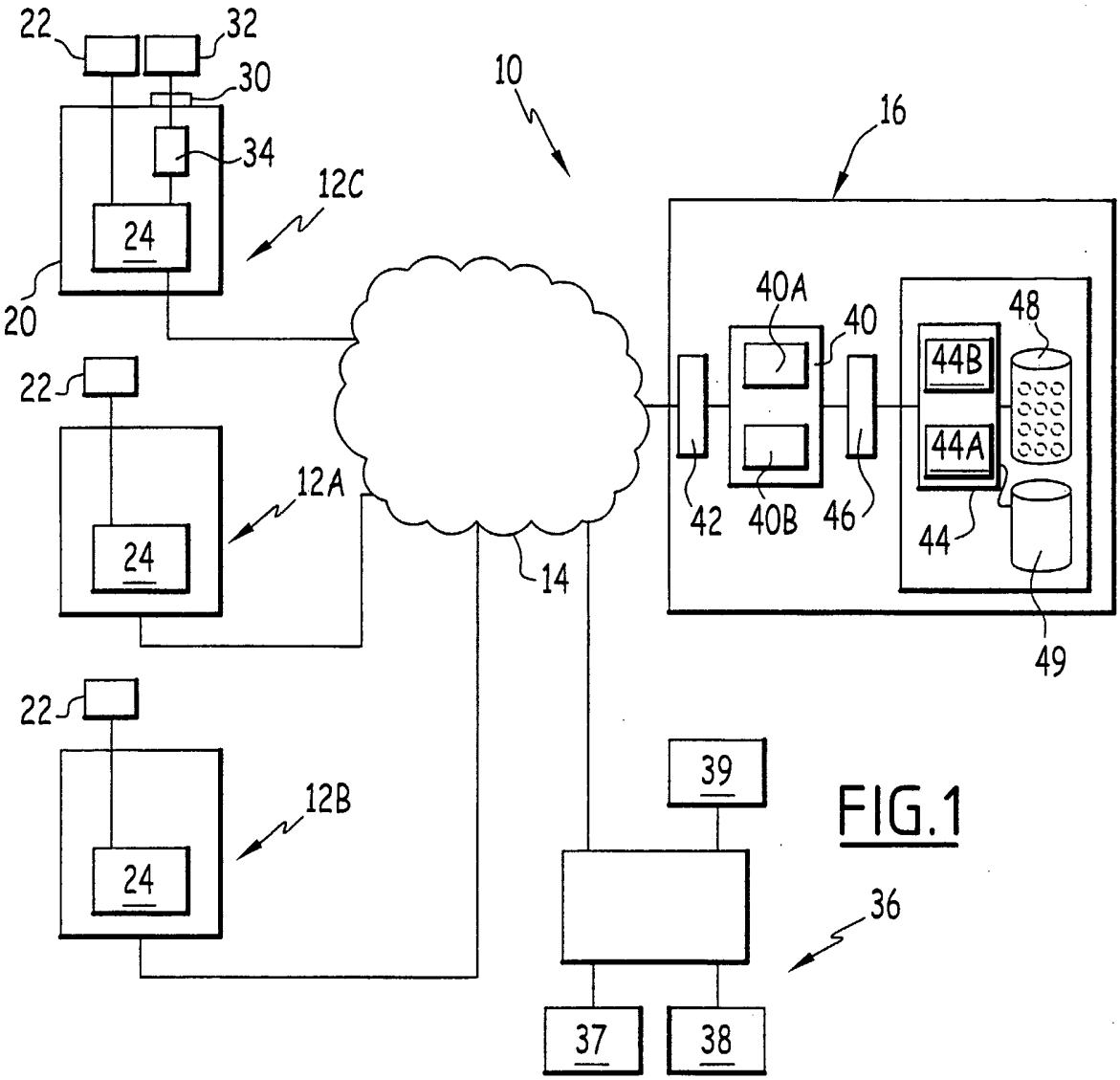

22
32
30
34
24
12C
20
10
16
40A
40
48
44B
44A
42
40B
46
44
49
22
12A
14
22
12B
39
36
37
38

FIG.1

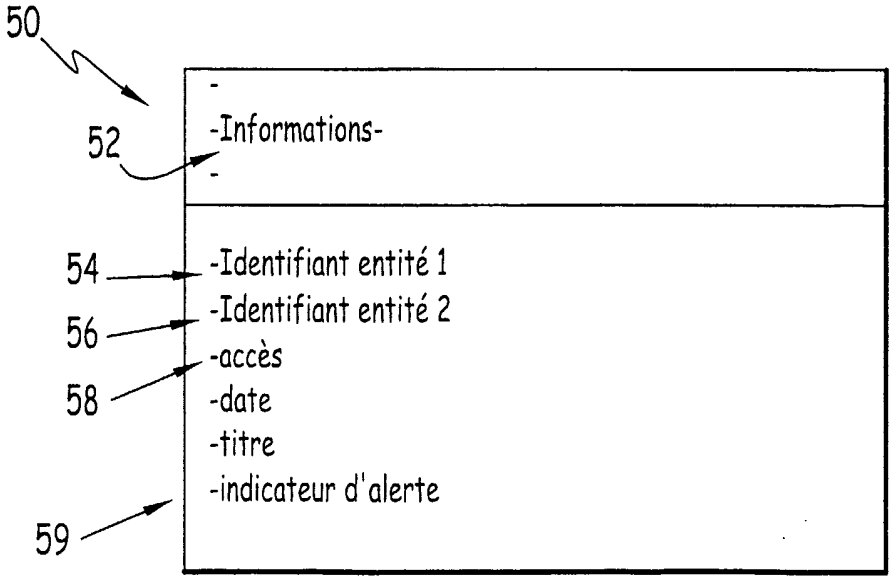

50
52
-Informations-
54
-Identifiant entité 1
56
-Identifiant entité 2
58
-accès
-date
-titre
-indicateur d'alerte
59

FIG.2

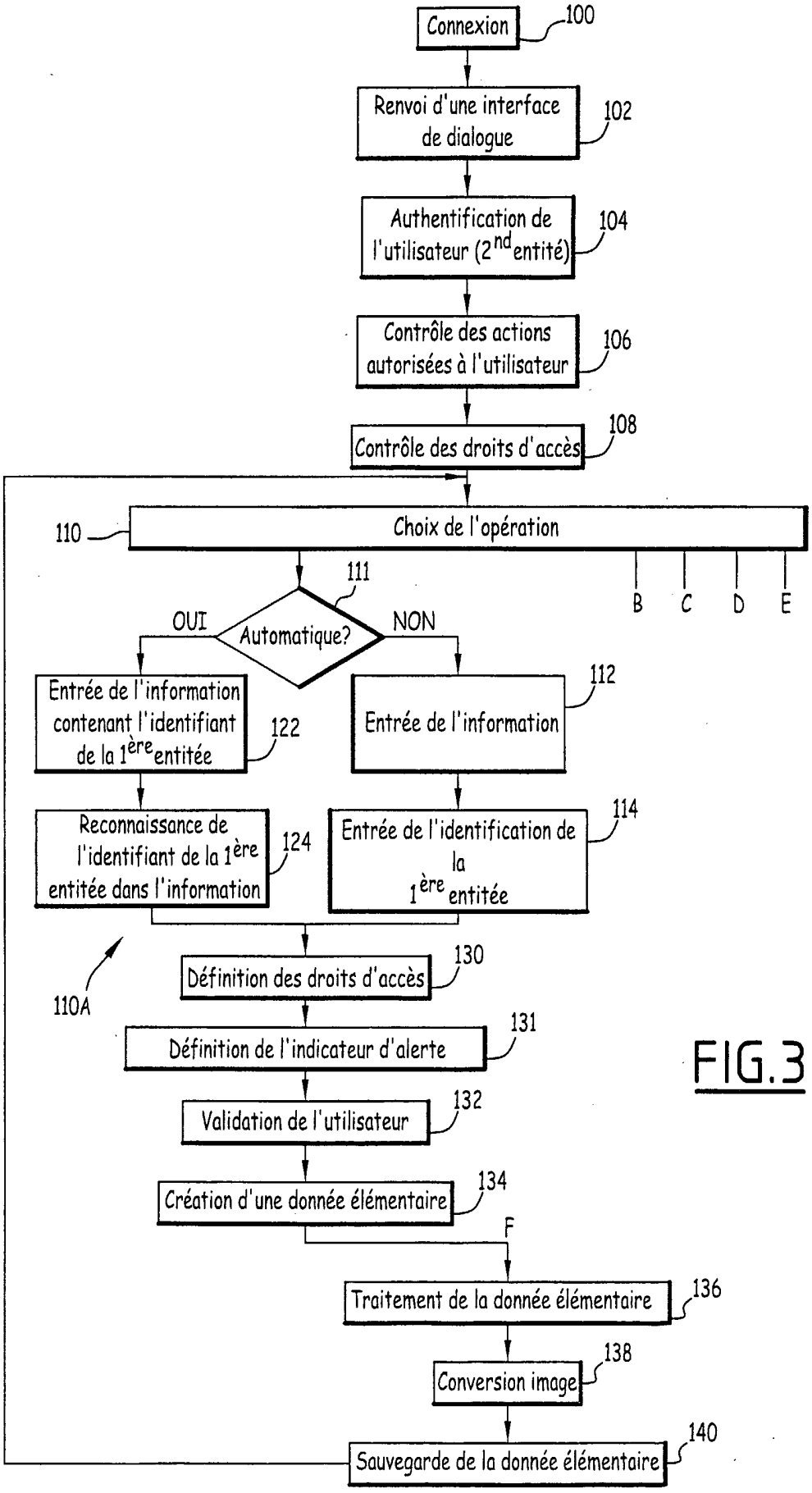

Connexion
100
Renvoi d'une interface de dialogue
102
Authentification de l'utilisateur (2nd entité)
104
Contrôle des actions autorisées à l'utilisateur
106
Contrôle des droits d'accès
108
110
Choix de l'opération
B
C
D
E
111
Automatique?
OUI
NON
Entrée de l'information contenant l'identifiant de la 1ère entitée
122
Entrée de l'information
112
Reconnaissance de l'identifiant de la 1ère entitée dans l'information
124
Entrée de l'identification de la 1ère entitée
114
110A
Définition des droits d'accès
130
Définition de l'indicateur d'alerte
131
Validation de l'utilisateur
132
Création d'une donnée élémentaire
134
F
Traitement de la donnée élémentaire
136
Conversion image
138
Sauvegarde de la donnée élémentaire
140

FIG.3

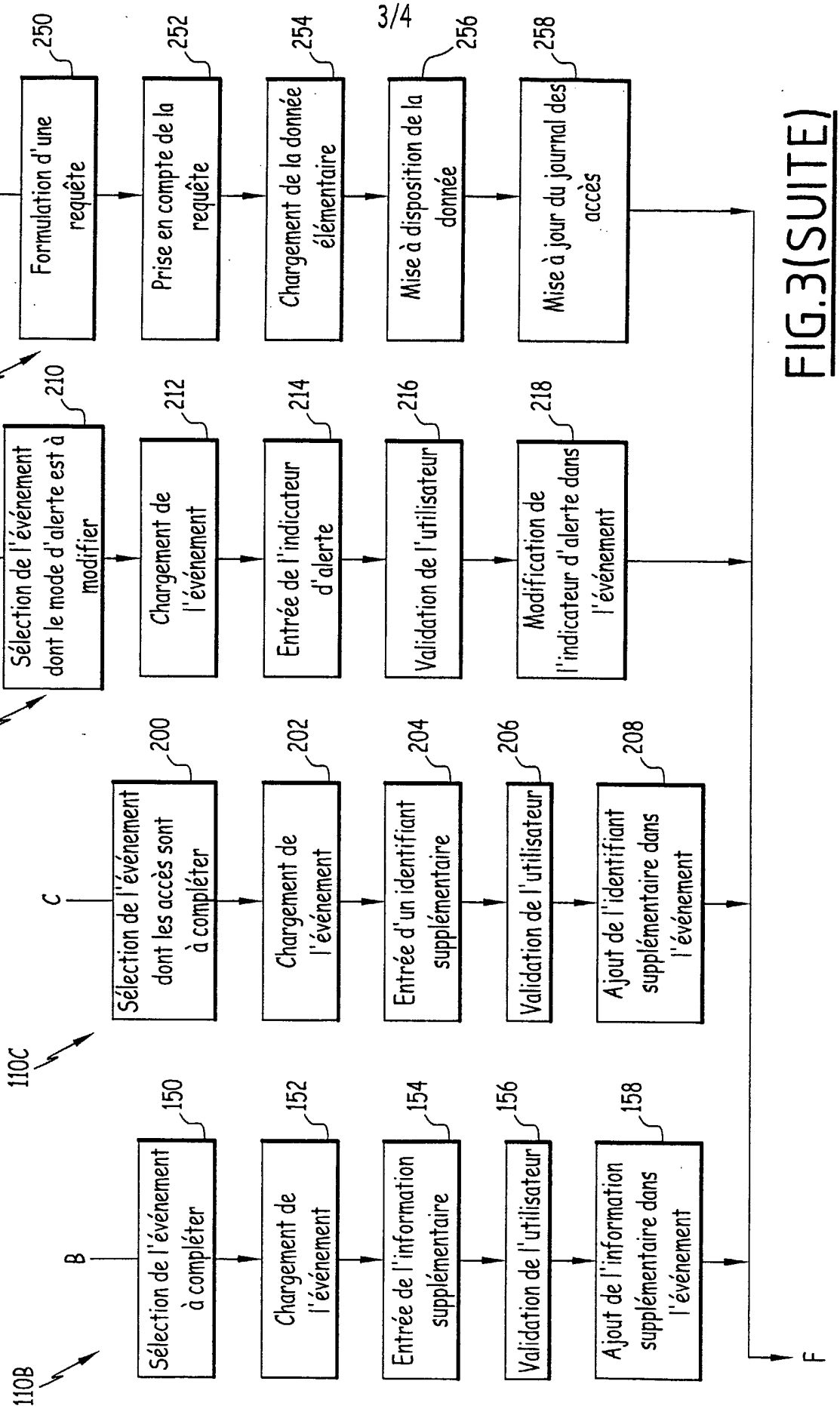

110B
B
Sélection de l'événement à compléter
150
Chargement de l'événement
152
Entrée de l'information supplémentaire
154
Validation de l'utilisateur
156
Ajout de l'information supplémentaire dans l'événement
158
110C
C
Sélection de l'événement dont les accès sont à compléter
200
Chargement de l'événement
202
Entrée d'un identifiant supplémentaire
204
Validation de l'utilisateur
206
Ajout de l'identifiant supplémentaire dans l'événement
208
110D
D
Sélection de l'événement dont le mode d'alerte est à modifier
210
Chargement de l'événement
212
Entrée de l'indicateur d'alerte
214
Validation de l'utilisateur
216
Modification de l'indicateur d'alerte dans l'événement
218
110E
E
Formulation d'une requête
250
Prise en compte de la requête
252
Chargement de la donnée élémentaire
254
Mise à disposition de la donnée
256
Mise à jour du journal des accès
258
F

FIG.3(SUITE)

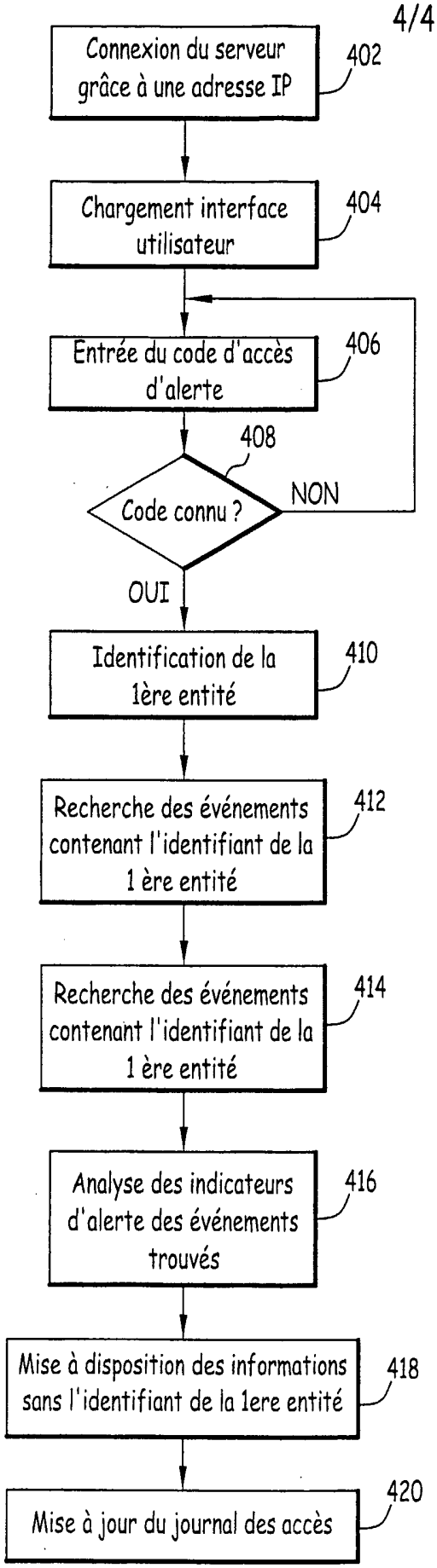

Connexion du serveur grâce à une adresse IP
402
Chargement interface utilisateur
404
Entrée du code d'accès d'alerte
406
408
Code connu ?
NON
OUI
Identification de la 1ère entité
410
Recherche des événements contenant l'identifiant de la 1 ère entité
412
Recherche des événements contenant l'identifiant de la 1 ère entité
414
Analyse des indicateurs d'alerte des événements trouvés
416
Mise à disposition des informations sans l'identifiant de la 1ere entité
418
Mise à jour du journal des accès
420

FIG.4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01665

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 63538 A (CAREKEY COM INC) 30 August 2001 (2001-08-30) abstract page 3, line 29 -page 4, line 6 page 4, line 23 -page 5, line 7 page 8, line 15 -page 8, line 19 page 9, line 1 -page 9, line 2 figure 2 ---	1-7
X	WO 01 55949 A (MIJNHARDT JAN ELI HENDRIK ;MEDLOOK NV (NL); RAUWERDINK WIM (NL)) 2 August 2001 (2001-08-02) page 2, line 3 -page 2, line 4 page 2, line 10 -page 2, line 18 page 3, line 6 -page 3, line 12 page 6, line 20 -page 7, line 6 page 7, line 26 -page 7, line 33 --- -/--	1-7

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 2003	16/10/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Segura, G

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01665

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 073 106 A (CHESKO KAREN L ET AL) 6 June 2000 (2000-06-06) column 4, line 33 -column 5, line 11 column 7, line 1 -column 7, line 14 column 9, line 25 -column 9, line 30 ---	1-7
A	WO 01 69514 A (EMEDICALFILES COM LLC) 20 September 2001 (2001-09-20) page 2, line 26 -page 3, line 19 page 7, line 7 -page 7, line 13 page 8, line 15 page 13, line 10 -page 13, line 19 ---	1-7
A	FR 2 704 336 A (ZEMMOUR JEAN CLAUDE) 28 October 1994 (1994-10-28) page 3, line 14 -page 4, line 6 -----	1-7

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/FR 03/01665

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0163538 A	30-08-2001	US 6463417 B1	08-10-2002
		AU 4723101 A	03-09-2001
		CA 2400160 A1	30-08-2001
		EP 1269378 A1	02-01-2003
		JP 2003524269 T	12-08-2003
		WO 0163538 A1	30-08-2001
WO 0155949 A	02-08-2001	WO 0155949 A1	02-08-2001
		AU 2467900 A	07-08-2001
US 6073106 A	06-06-2000	NONE	
WO 0169514 A	20-09-2001	AU 4367301 A	24-09-2001
		EP 1297478 A2	02-04-2003
		WO 0169514 A2	20-09-2001
FR 2704336 A	28-10-1994	FR 2704336 A1	28-10-1994
		EP 0647339 A1	12-04-1995
		WO 9424630 A1	27-10-1994

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/01665

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00 G06F19/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 01 63538 A (CAREKEY COM INC) 30 août 2001 (2001-08-30) abrégé page 3, ligne 29 -page 4, ligne 6 page 4, ligne 23 -page 5, ligne 7 page 8, ligne 15 -page 8, ligne 19 page 9, ligne 1 -page 9, ligne 2 figure 2 ---	1-7
X	WO 01 55949 A (MIJNHARDT JAN ELI HENDRIK ;MEDLOOK NV (NL); RAUWERDINK WIM (NL)) 2 août 2001 (2001-08-02) page 2, ligne 3 -page 2, ligne 4 page 2, ligne 10 -page 2, ligne 18 page 3, ligne 6 -page 3, ligne 12 page 6, ligne 20 -page 7, ligne 6 page 7, ligne 26 -page 7, ligne 33 --- -/--	1-7

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 octobre 2003	16/10/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Segura, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/01665

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	US 6 073 106 A (CHESKO KAREN L ET AL) 6 juin 2000 (2000-06-06) colonne 4, ligne 33 -colonne 5, ligne 11 colonne 7, ligne 1 -colonne 7, ligne 14 colonne 9, ligne 25 -colonne 9, ligne 30 ---	1-7
A	WO 01 69514 A (EMEDICALFILES COM LLC) 20 septembre 2001 (2001-09-20) page 2, ligne 26 -page 3, ligne 19 page 7, ligne 7 -page 7, ligne 13 page 8, ligne 15 page 13, ligne 10 -page 13, ligne 19 ---	1-7
A	FR 2 704 336 A (ZEMMOUR JEAN CLAUDE) 28 octobre 1994 (1994-10-28) page 3, ligne 14 -page 4, ligne 6 -----	1-7

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/01665

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0163538	A	30-08-2001	US	6463417 B1	08-10-2002
			AU	4723101 A	03-09-2001
			CA	2400160 A1	30-08-2001
			EP	1269378 A1	02-01-2003
			JP	2003524269 T	12-08-2003
			WO	0163538 A1	30-08-2001
WO 0155949	A	02-08-2001	WO	0155949 A1	02-08-2001
			AU	2467900 A	07-08-2001
US 6073106	A	06-06-2000	AUCUN		
WO 0169514	A	20-09-2001	AU	4367301 A	24-09-2001
			EP	1297478 A2	02-04-2003
			WO	0169514 A2	20-09-2001
FR 2704336	A	28-10-1994	FR	2704336 A1	28-10-1994
			EP	0647339 A1	12-04-1995
			WO	9424630 A1	27-10-1994