

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
24. Juli 2003 (24.07.2003)

PCT

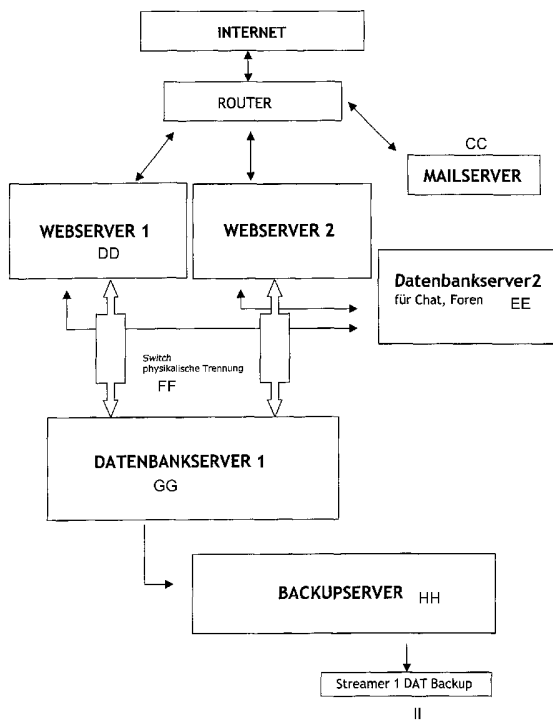
(10) Internationale Veröffentlichungsnummer
WO 03/060803 A2

- (51) Internationale Patentklassifikation⁷: G06F 19/00 (74) Anwälte: LUCHT, Silvia usw.; Kaiser-Joseph-Strasse, 79098 Freiburg (DE).
- (21) Internationales Aktenzeichen: PCT/EP03/00364
- (22) Internationales Anmeldedatum: 15. Januar 2003 (15.01.2003) (81) Bestimmungsstaat (national): US.
- (25) Einreichungssprache: Deutsch (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität: 102 01 257.1 15. Januar 2002 (15.01.2002) DE — ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts
- (71) Anmelder und
(72) Erfinder: BAUER, Karl-Heinz [CH/CH]; Im Schwizergut 25, CH-8610 Uster (CH).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR SECURING PATIENT DATA

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR SICHERUNG VON PATIENTENDATEN



(57) Abstract: The invention relates to a method and device for securing patient data when exchanging information between a patient and a specialist via a data network using computers. The invention involves the use of a first web server, which serves to exchange data pertaining to the individual who is the patient, and of a second web server, which serves to exchange data pertaining to the ailments of the patient.

(57) Zusammenfassung: Es werden ein Verfahren und eine Vorrichtung zur Sicherung von Patientendaten bei einem Austausch von Informationen zwischen einem Patienten und einem Fachmann durch ein Datennetzwerk mit Hilfe von Computern vorgeschlagen, bei denen ein erster Webserver für den Austausch von Daten betreffend die Person des Patienten und ein zweiter Webserver für den Austausch von Daten betreffend die Beschwerden des Patienten vorgesehen sind.

CC... MAIL SERVER
DD... WEB SERVER
EE... DATABASE SERVER 2 FOR CHATTING, FORUMS
FF... SWITCH PHYSICAL SEPARATION
GG... DATABASE SERVER 1
HH... BACK UP SERVER
II... STREAMER 1 DAT BACKUP



WO 03/060803 A2



Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und Vorrichtung zur Sicherung von Patientendaten

Beschreibung

Die Erfindung geht aus von einem Verfahren und einer Vorrichtung zur Sicherung von Patientendaten bei einem Austausch von Informationen nach dem Oberbegriff des Anspruchs 1 und des Anspruchs 6.

Sofern eine Person medizinische Ratschläge eines Fachmannes, beispielsweise eines Arztes wünscht, so muss sie sich bei dem betreffenden Fachmann einen Termin geben lassen und die Symptome ihrer Krankheit in einem persönlichen Gespräch mit dem Arzt erörtern. In der Regel ist es für den Patienten nicht möglich, umgehend eine Antwort auf seine Fragen zu erhalten, wenn die Beschwerden auftreten. Eine telefonische Auskunft erhält er normalerweise nicht. Hat die Person keine akuten Beschwerden und interessiert sich lediglich für eine medizinische Fragestellung, so kann sie nur in der medizinischen Fachliteratur nach einer Antwort suchen.

Der Austausch von Patientendaten zwischen Fachpersonen, beispielsweise Ärzte oder Therapeuten, findet in persönlichen Gesprächen oder auf schriftlichem Weg statt. Ein Austausch mit Hilfe eines Computernetzwerkes genügt nicht den erhöhten Sicherheitsanforderungen, da nicht ausgeschlossen werden kann, dass Dritte von den Daten Kenntnis erlangen.

Diese Nachteile führen dazu, dass die Kombination aus Telekommunikation und Informatik, abgekürzt Telematik im Gesundheitswesen keine Anwendung findet.

Demgegenüber bieten das erfindungsgemäße Verfahren mit den kennzeichnenden Merkmalen des Anspruchs 1 und die erfindungsgemäße Vorrichtung mit den kennzeichnenden Merkmalen des Anspruchs 6 den Vorteil, dass Patientendaten über ein Datennetzwerk, beispielsweise das Internet, ausgetauscht werden können, ohne dass dabei die Gefahr besteht, dass Dritte unerlaubt von den Daten Kenntnis erlangen können. So kann beispielsweise ein Patient eine Anfrage an Fachleute im medizinischen Bereich richten. Dabei werden die Patientendaten vollständig anonymisiert, um die Sicherheit und Vertraulichkeit der übermittelten Daten zu gewährleisten. Der Benutzer oder Patient gibt über ein Formular die von ihm benötigten Angaben, beispielsweise seinen Namen, die Anschrift und evtl. seine Bankverbindung an. Angaben zu seinen Beschwerden oder seiner Krankheit kann der Patient hier nicht eintragen. Derartige Eingaben werden durch vorgegebene Felder in dem Formular unterdrückt. Nachdem der Patient seine Daten eingegeben hat, wird ihm durch den Webserver und/ oder den Datenbankserver eine Identifikationsnummer zugeteilt. Unter dieser Identifikationsnummer wird für den Patienten ein Postfach eingerichtet, das für einen bestimmten Zeitraum benutzt werden kann. Nach Ablauf einer vorgegebenen Zeit werden die Identifikationsnummer und das zugehörige Postfach aus Sicherheitsgründen gelöscht. Sofern der Patient eine Anfrage an einen Fachmann richten möchte, so muss er in einem zweiten Formular zunächst seine Identifikationsnummer angeben und anschließend die Anfrage eingeben. Hierzu benötigt der Patient keine Email-Adresse. Es ist ausreichend, dass der Patient über einen Internetzugang verfügt. Sobald der Patient seine Abfrage abgeschickt hat, kann überprüft werden, ob die angegebene Identifikationsnummer gültig ist und, sofern eine Bezahlung verlangt wird, ob der Patient bereits für seine Anfrage bezahlt hat. Sofern die Identifikationsnummer gültig und eine Bezahlung erfolgt ist, wird die Anfrage an einen Fachmann weitergeleitet und durch diesen beantwortet. Die Antwort wird in dem unter der Identifikationsnummer geführten Postfach abgelegt und kann durch den Patienten bei Eingabe seiner Identifikationsnummer abgefragt werden. Die Antwort erscheint in diesem Fall aus Sicherheitsgründen in einem unsichtbaren Frame-Set. Dadurch ist dem Benutzer die Möglichkeit

genommen, in die Adresszeile direkt eine URL-Adresse einzugeben und somit sich unerwünscht Daten beschaffen zu können, welche auf den Servern abgelegt sind.

Durch die strikte Trennung der Daten betreffend die Person des Patienten und seiner Anfrage kann gewährleistet werden, dass die Patientendaten ausreichend geschützt sind und nicht unbefugt oder unberechtigt eingesehen werden können.

Zur Trennung der Daten zur Person einerseits und der Daten betreffend die Anfrage andererseits sind ein erster Webserver für die Personendaten und ein zweiter Webserver für die Daten der Anfrage vorgesehen. Jeder der beiden Webserver ist über einen Router mit dem Internet verbunden. Erster und zweiter Webserver sind mit Datenbankservern verbunden. Dabei kann es sich um einen oder mehrere Datenbankserver handeln. Der erste Webserver und der zweite Webserver sind vollständig entkoppelt.

Zwischen den Webservern und dem Datenbankserver ist eine physikalische Trennung vorgesehen. Auf diese Weise wird verhindert, dass sich Dritte über das Internet unberechtigten Zugang auf die Daten des Datenbankservers verschaffen.

Um die Datensicherheit zu erhöhen werden die Daten des Datenbankservers in regelmäßigen, zeitlichen Abständen auf einem externen Datenträger gespeichert und die auf dem Datenbankserver vorhandenen Daten gelöscht. Werden die Inhalte des Datenbankservers durch Dritte unberechtigt gelesen, so besteht in diesem Fall lediglich Zugriff auf die seit der letzten Datensicherung angefallenen Daten. Ein geeigneter Zeitraum für die Erstellung von Datensicherungen sind beispielsweise 48 Stunden.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung können zur weiteren Erhöhung der Datensicherheit die Daten vor dem Versenden Verschlüsselt und nach dem Empfang wieder entschlüsselt werden. Hierzu

eignen sich bekannte Verfahren der Datenverschlüsselung und der Kryptografie. Die erfindungsgemäße Vorrichtung kann zur Ver- und Entschlüsselung mit einem Kryptomodul ausgestattet sein.

Die auf dem zweiten Webserver und dem Datenbankserver vorhandenen Daten müssen nicht durch aufwendige Datensicherungen entsprechend abgesichert werden, da sie lediglich die Identifikationsnummer und die Anfragen sowie die Antworten zu den einzelnen Fällen enthalten. Bei einem Zugriff durch Unberechtigte können diese Daten keinen bestimmten Personen zugeordnet werden. Die Daten müssen daher nicht stärker geschützt werden als eine normale Mailingliste. Dagegen werden die Daten des ersten Webservers stärker geschützt, da sie Personendaten und eventuell Bankverbindungen enthalten.

Dank dieser erhöhten Sicherung der Patientendaten kann die Telematik auch im Gesundheitswesen Anwendung finden. Telediagnose, Telepathologie, Teletherapie und Telematik in der ambulanten Pflege werden auf diese Weise ermöglicht. Der Austausch der Patientendaten kann nicht nur zwischen Patient und Arzt sondern auch zwischen Ärzten, Therapeuten oder sonstigen Fachleuten stattfinden. Fachleute können Patienten an andere Fachärzte vermitteln oder ihr Wissen auf dem aktuellen Stand halten. Daten, die sich nicht auf einen Patienten beziehen, können in einer für die Nutzer frei zugänglichen Datenbank zur Verfügung gestellt werden. Derartige Wissensdatenbanken werden im Bereich der medizinischen Versorgung eine bedeutende Rolle spielen. Die Vernetzung medizinischer Versorgungsstrukturen führt zu einer verbesserten und erleichterten Betreuung des Patienten. Arztbesuche oder Krankenhausaufenthalte können unter Umständen vermieden werden. Das Datennetz kann in mehrere Segmente unterteilt sein, die jeweils die unterschiedlichen Interessen verschiedener Zielgruppen berücksichtigen.

Für Ärzte ist die Teilnahme an einer derartigen Plattform in einem Datennetz mit einer Vielzahl von Vorteilen verbunden. Behandlungskapazitäten können

besser ausgelastet werden. Aktuelle Informationen verbessern die bei der täglichen Arbeit notwendigen Kenntnisse. Der Arzt kann eine Beratung hinsichtlich der Praxisverwaltung, von Benchmarking, Consulting und separaten Verträgen mit Krankenkassen erhalten. Fachärzte können sich zu Gruppen zusammenschließen. Als Gruppe haben die Ärzte insbesondere gegenüber Krankenkassen, der Industrie und dem Gesetzgeber entscheidende Vorteile. Außerdem können beim Einkauf von Praxisbedarf Rabatte erreicht werden.

Patienten haben die Möglichkeit, sich über das Datennetz zu Selbsthilfegruppen zusammenzuschließen. Erfahrungen, Kenntnisse und Krankheitsbilder können ausgetauscht werden. Hierzu können die Patienten freiwillig ihre Identität preisgeben. Dies ist jedoch nicht notwendig.

Nach einer vorteilhaften Ausgestaltung der Erfindung sind ein erster und zweiter Datenbankserver vorgesehen, welche beide sowohl mit dem ersten als auch mit dem zweiten Webserver verbunden sind. Diese Trennung zwischen erstem und zweitem Webserver einerseits und erstem und zweitem Datenbankserver andererseits erhöht nicht nur die Sicherheit bezüglich unberechtigter Zugriffe auf die Daten sondern sorgt auch dafür, dass das System selbst beim Ausfall eines Servers noch funktionsfähig ist.

Das zweite Formular zur Eingabe der Anfrage kann dem Patienten eine Vorauswahl verschiedener Themenbereiche anzeigen. Damit wird der Patient aufgefordert, seine Anfrage einem bestimmten Sachgebiet zuzuordnen. Dies erleichtert die Beantwortung der Fragen. Da die Antworten sehr allgemein abgefasst sein müssen und keine individuellen Informationen berücksichtigen dürfen, kann die Beantwortung automatisiert werden. Die von den Fachleuten, beispielsweise Ärzten, erstellten Antworten werden in einer Datenbank abgelegt und einem definierten Krankheitsbild zugeordnet. Bei einer Anfrage eines Patienten genügt es, das Krankheitsbild zu definieren und die in der Datenbank abgelegten Antworten abzurufen. Dadurch wird der redaktionelle Aufwand stark minimiert.

Weitere Vorteile und vorteilhafte Ausgestaltungen der Erfindung sind der nachfolgenden Beschreibung, der Zeichnung und den Ansprüchen entnehmbar.

Zeichnung

In der Zeichnung ist ein Ausführungsbeispiel der Erfindung dargestellt und im folgenden näher beschrieben. Es zeigt:

Figur 1 schematische Darstellung der verschiedenen Komponenten der erfindungsgemäßen Vorrichtung.

Beschreibung des Ausführungsbeispiels

Die Daten des Patienten sowie seine Anfrage und die Antwort werden mit Hilfe des Internets ausgetauscht. An der Schnittstelle zwischen dem Internet und der Vorrichtung befindet sich der Router. Von dort gelangen die Daten betreffend die Person des Patienten wie beispielsweise Namen und Anschrift zum ersten Webserver und weiter zum ersten Datenbankserver. Der erste Datenbankserver ordnet dem Patienten eine Identifikationsnummer zu und leitet sie über den ersten Webserver und das Internet an den Patienten weiter. Die Anfragen mit der zugehörigen Identifikationsnummer, sowie die Antworten werden über den zweiten Webserver ausgetauscht und abgelegt. Aus der Darstellung ist erkennbar, dass der erste und der zweite Webserver, sowie der erste und der zweite Datenbankserver vollständig entkoppelt sind. Der zweite Datenbankserver dient hauptsächlich für Gesprächsrunden oder Foren. Sofern der erste Datenbankserver ausfällt kann der zweite Datenbankserver dessen Aufgaben übernehmen.

Um die Sicherheit zu erhöhen sind zwischen den beiden Webservern und dem Datenbankservern physikalische Trennungen vorgesehen.

Über einen Backupserver werden mit Hilfe von Streamern Sicherungskopien der Daten erstellt. Der über den Router mit dem Internet verbundene Mailserver dient dazu weitere Daten, wie beispielsweise Artikel zu bestimmten Themen, Empfehlungen zur Ernährung oder zur sportlichen Betätigung zu übermitteln. Dieser Datenaustausch erfolgt über e-mail.

Alle in der Beschreibung, den nachfolgenden Ansprüchen und der Zeichnung dargestellten Merkmale können sowohl einzeln als auch in beliebiger Kombination miteinander erfindungswesentlich sein.

Ansprüche

1. Verfahren zur Sicherung von Patientendaten bei einem Austausch von Informationen durch ein Datennetzwerk mit Hilfe von Computern, dadurch gekennzeichnet, dass Name und Anschrift des Patienten in ein auf einem Bildschirm eines Computers angezeigtes erstes Formular eingegeben werden, dass dem Patienten eine Identifikations-Nummer zugeordnet und auf dem Bildschirm angezeigt wird, dass die Identifikationsnummer und eine Anfrage in ein auf einem Bildschirm angezeigtes zweites Formular eingegeben werden, dass die Antwort auf die Anfrage der Identifikations-Nummer zugeordnet und bei Angabe der Identifikations-Nummer auf einem Bildschirm angezeigt wird.
2. Verfahren nach Anspruch 1, dass der Name und die Anschrift des Patienten einerseits und die Anfrage und die Antwort andererseits in getrennten Webservern und/ oder getrennten Datenbankservern bearbeitet und gespeichert werden.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Identifikations-Nummer nach Ablauf einer vorgegebenen Zeit gelöscht wird.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der auf einem Webserver und/ oder Datenbankserver abgelegte Name und die Anschrift des Patienten nach Ablauf einer vorgegebenen Zeit auf einem externen Datenträger gespeichert und auf dem Webserver und/ oder Datenbankserver gelöscht wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Daten vor dem Versenden verschlüsselt werden und nach dem Empfang wieder entschlüsselt werden.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Antwort in einem unsichtbaren Frame-Set angezeigt wird.
7. Vorrichtung zur Sicherung von Patientendaten bei einem Austausch von Informationen zwischen einem Patienten und einem Fachmann mithilfe eines Datennetzwerkes, insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass ein erster Webserver und ein mit dem ersten Webserver verbundener Datenbankserver vorgesehen sind, über die der Name und die Anschrift des Patienten angegeben und abgespeichert werden, und über die dem Patienten eine Identifikations-Nummer zugeteilt wird, dass ein zweiter Webserver vorgesehen ist, über den der Patient unter seiner Nummer Daten mit einem Fachmann austauschen kann, dass der zweite Webserver mit dem Datenbankserver verbunden ist, und dass der erste Webserver und der zweite Webserver entkoppelt sind.
8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass zwischen dem ersten Webserver und dem Datenbankserver einerseits und zwischen dem zweiten Webserver und dem Datenbankserver andererseits physikalische Trennungen vorgesehen sind.
9. Vorrichtung nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass ein zweiter Datenbankserver vorgesehen ist, welcher mit dem ersten und/oder mit dem zweiten Webserver verbunden ist.
10. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass eine Datensicherungseinheit vorgesehen ist, welche die Daten des

Datenbankservers in regelmäßigen zeitlichen Abständen auf einem externen Datenspeicher speichert und die Daten des Datenbankservers löscht.

11. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass ein Kryptomodul zum Verschlüsseln und Entschlüsseln der Daten vorgesehen ist.

Figur 1

