

(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
29. August 2013 (29.08.2013)



(10) Internationale Veröffentlichungsnummer
WO 2013/124014 A1

(51) Internationale Patentklassifikation:
G06Q 10/10 (2012.01)

(21) Internationales Aktenzeichen: PCT/EP2012/074334

(22) Internationales Anmeldedatum:
4. Dezember 2012 (04.12.2012)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 202 701.7
22. Februar 2012 (22.02.2012) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
[DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **FRIESE, Thomas**; Oberölkofener Straße 9,
81671 München (DE). **GOSSLER, Thomas**; Pfälzer Str.
24, 91052 Erlangen (DE).

DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,
KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ,
TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ,
TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,
RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT,
LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,
SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA,
GN, GQ, GW, ML, MR, NE, SN, TD, TG).

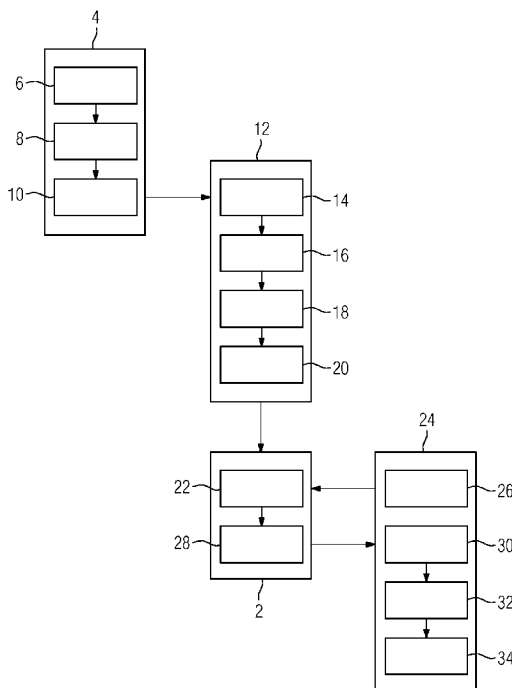
Veröffentlicht:

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,
BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK,

— mit internationalem Recherchenbericht (Artikel 21 Absatz
3)

(54) Title: METHOD FOR PROCESSING PATIENT-BASED DATA SETS

(54) Bezeichnung : VERFAHREN ZUR BEARBEITUNG VON PATIENTENBEZOGENEN DATENSÄTZEN



(57) Abstract: The invention relates to a method for processing patient-based data sets, which each comprise medical data and sensitive patient data as plain data, wherein the sensitive patient data of each patient-based data sets are anonymized (20) whereby anonymized patient-based data sets are generated, test data from each patient-based data set is generated from the respective sensitive patient data and incorporated in the respective patient-based data set (18) by means of an algorithm, the anonymized patient-based data sets together with the test data are made available in a cloud computing architecture (2), sensitive patient data about a selected patient is predefined within the context of processing a specific patient-based data set on a client computer (24) that is attached to the cloud computing architecture (2) and enquiry data is generated from said predefined sensitive patient data (26) by means of the algorithm, and a security function is triggered if the test data from the specific patient-based data set does not agree with the enquiry data about the selected patient.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Bearbeitung von patientenbezogenen Datensätzen, die jeweils medizinische Daten und sensitive Patientendaten als Klardaten umfassen, bei dem die sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes anonymisiert werden (20), wodurch anonymisierte patientenbezogene Datensätze erzeugt werden, bei dem mit Hilfe eines Algorithmus aus den jeweiligen

[Fortsetzung auf der nächsten Seite]



sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes Prüfdaten generiert und in dem jeweiligen patientenbezogenen Datensatz eingebunden werden (18), bei dem die anonymisierten patientenbezogenen Datensätze mit den Prüfdaten in einer Cloud- Computing-Architektur (2) zur Verfügung gestellt werden (22), bei dem an einem Clientrechner (24), der an die Cloud- Computing-Architektur (2) angebunden ist, im Rahmen einer Bearbeitung eines bestimmten patientenbezogenen Datensatzes sensitive Patientendaten eines ausgewählten Patienten vorgegeben werden und bei dem mit Hilfe des Algorithmus aus diesen vorgegeben sensitiven Patientendaten Abfragedaten generiert werden (26) und bei dem eine Sicherungsfunktion ausgelöst wird, wenn die Prüfdaten des bestimmten patientenbezogenen Datensatzes nicht mit den Abfragedaten des ausgewählten Patienten übereinstimmen.

Beschreibung

Verfahren zur Bearbeitung von patientenbezogenen Datensätzen

- 5 Die Erfindung betrifft ein Verfahren zur Bearbeitung von patientenbezogenen Datensätzen, die jeweils medizinische Daten und sensitive Patientendaten als Klardaten umfassen.

Aktuelle Entwicklungen im Medizinbereich zielen darauf ab,
10 ein zentrales Informationstechnologie-System zu schaffen, mit dessen Hilfe die medizinischen Daten eines jeden Patienten zusammengetragen und derart archiviert werden, dass jeder vom Patienten bestimmte Mediziner die Möglichkeit hat, einfach und schnell auf alle von ihm benötigten medizinischen Daten
15 des Patienten zuzugreifen.

Dazu ist es notwendig medizinische Daten des Patienten aus dem unmittelbaren Kontrollbereich einzelner medizinischer Einrichtungen heraus in eine von mehreren Nutzern gemeinsam
20 verwendete Cloud-Computing-Architektur zu übertragen. Hierbei ist es wünschenswert oder, aufgrund gesetzlicher Regelungen, häufig auch notwendig, dass die sogenannten „Protected Health Information“ (PHI), also alle Daten, die den Patienten eindeutig identifizierbar machen, aus den medizinischen Daten
25 des Patienten entfernt werden. Dies gilt beispielsweise auch für Daten, die nach dem DICOM-Standard (Digital Imaging and Communications in Medicine) ausgebaut sind und die Bilddaten enthalten, welche beispielsweise bei Untersuchungen mittels eines Computertomographen erstellt werden. Die Anonymisierung
30 der „Protected Health Information“ kann dabei z.B. auch durch Pseudonym-Vergabe erfolgen, sofern das Pseudonym nur dem Urheber der Daten, also der jeweiligen medizinischen Einrichtung, bekannt ist.

35 Um die Patientensicherheit zu gewährleisten und insbesondere um Fehldiagnosen zu vermeiden besteht zudem die Forderung, dass bei der Generierung von Bilddaten im Rahmen einer Untersuchung mittels eines bilderzeugenden medizinischen Systems

die Patientenidentität untrennbar mit den generierten Bilddaten verknüpft wird, sodass eine fehlerhafte Zuordnung von Bilddaten zu einem Patienten möglichst ausgeschlossen wird.

5 Aufgrund dieser beiden widersprüchlichen Anforderungen wurde bisher meist auf den Einsatz von Cloud-Computing-Architekturen, welche eine Vielzahl von Nutzern gemeinsam verwenden, verzichtet oder aber die Cloud-Computing-Architektur wurde mitsamt allen Zugängen im Kontrollbereich einer einzelnen medizinischen Einrichtung angesiedelt, da in diesem Fall eine Anonymisierung der „Protected Health Information“ nicht notwendig ist. Bei einer anderen häufig verwendeten Lösung werden lediglich verschlüsselte Daten an die Cloud-Computing-Architektur abgegeben und in dieser zur Verfügung gestellt, wobei eine Entschlüsselung der Daten durch eine lokal beim Nutzer installierte Client-Application ermöglicht wird. Je nach Datenmenge und Art der Verschlüsselung ist mit einer entsprechenden Verschlüsselung der Daten oder Entschlüsselung der Daten ein sehr großer Rechenaufwand verbunden. Da die Daten für die Weiterverarbeitung in der Regel entschlüsselt vorliegen müssen, ist es in diesem Fall außerdem notwendig jeweils den gesamten Datensatz zu übertragen. Daher ist diese Lösung insbesondere bei Bilddaten und/oder im Falle von Nutzerzugängen, bei denen lokal nur eine relativ geringe Rechenleistung gegeben ist, und/oder bei Netzwerken, bei denen einige Netzwerkverbindungen eine relativ geringe Bandbreite für die Datenübertragung aufweisen, unvorteilhaft.

Ausgehend hiervon liegt der Erfindung die Aufgabe zugrunde, ein alternatives und vorteilhaftes Verfahren zur Bearbeitung von patientenbezogenen Datensätzen anzugeben.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den Merkmalen des Anspruchs 1 gelöst. Die rückbezogenen Ansprüche beinhalten teilweise vorteilhafte und teilweise für sich selbst erfinderische Weiterbildungen dieser Erfindung.

Das Verfahren dient zur Bearbeitung von patientenbezogenen Datensätzen, die jeweils medizinische Daten und sensitive Patientendaten als Klardaten umfassen. Im Rahmen des Verfahrens werden die sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes anonymisiert, wodurch anonymisierte patientenbezogene Datensätze erzeugt werden. Weiter werden mit Hilfe eines Algorithmus aus den jeweiligen sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes Prüfdaten generiert und in den jeweiligen patientenbezogenen Datensatz eingebunden. Nachfolgend werden die anonymisierten patientenbezogenen Datensätze mit den Prüfdaten in einer Cloud-Computing-Architektur zur Verfügung gestellt. Zudem werden an einem Client-Rechner, der an die Cloud-Computing-Architektur angebunden ist, im Rahmen einer Bearbeitung eines bestimmten patientenbezogenen Datensatzes sensitive Patientendaten eines ausgewählten Patienten vorgegeben und mit Hilfe des Algorithmus werden aus diesen vorgegebenen sensitiven Patientendaten Abfragedaten generiert. Stimmen die Abfragedaten des ausgewählten Patienten nicht mit den Prüfdaten des bestimmten patientenbezogenen Datensatzes überein, so wird eine Sicherungsfunktion ausgelöst. Der Ausdruck patientenbezogene Datensätze steht dabei insbesondere für Dateien nach dem DICOM-Standard (Digital Imaging and Communications in Medicine) und der Ausdruck sensitive Patientendaten umfasst vor allem sogenannte „Protected Health Information“ (PHI).

Es werden bei diesem Verfahren also nicht die kompletten patientenbezogenen Datensätze verschlüsselt, sondern es werden lediglich einzelne darin enthaltene Informationen, nämlich die sensitiven Patientendaten, verschleiert. Dies geschieht beispielsweise, indem die sensitiven Patientendaten, wie der Name des Patienten, dessen Geburtsdatum usw. auf eine Art und Weise verschlüsselt werden, bei der die entsprechenden Klardaten durch geeignete Platzhalter ersetzt werden. Infolgedessen lassen sich die patientenbezogenen Datensätze auch nach der Anonymisierung der sensitiven Patientendaten weiterverarbeiten, ohne dass die Anonymisierung der sensitiven Patientendaten zuvor rückgängig gemacht werden muss. Dementspre-

chend können die anonymisierten patientenbezogenen Datensätze in der Cloud-Computing-Architektur zur Verfügung gestellt und in dieser gespeichert und/oder weiterverarbeitet werden, ohne dass die sensitiven Patientendaten innerhalb der Cloud-

5 Computing-Architektur als Klardaten auftreten. Außerdem verbleiben die sensitiven Patientendaten, wenn auch anonymisiert, fest in den patientenbezogenen Datensätze eingebunden, so dass die beiden eingangs genannten und widersprüchlichen Forderungen bei diesem Verfahren erfüllt werden. Zugang zu
10 den patientenbezogenen Datensätzen erhalten nur autorisierte Personen, insbesondere die vom jeweiligen Patienten ausgewählten Mediziner, denen die sensitiven Patientendaten als Klardaten bekannt sind und die Zugang zu einer Anwendung haben, mit deren Hilfe sie aus den Klardaten die anonymisierten
15 sensitiven Patientendaten, also insbesondere die Platzhalter, an einem Client-Rechner generieren können. Über diesen Client-Rechner, der an die Cloud-Computing-Architektur angebunden ist, erhalten sie dann Zugang zu den patientenbezogenen Datensätzen. Da hierbei lediglich ein Abgleich erfolgt, bei dem die am Client-Rechner generierten anonymisierten
20 sensitiven Patientendaten mit den anonymisierten sensitiven Patientendaten in den anonymisierten patientenbezogenen Datensätzen verglichen werden, tauchen auch bei einem Zugriff auf die Cloud-Computing-Architektur die Klardaten in dieser nicht
25 auf.

Zugunsten einer möglichst einfach gestalteten Datenverarbeitung, werden die anonymisierten sensitiven Patientendaten, also insbesondere die Platzhalter, zudem zur Bildung eines
30 zusätzlichen sogenannten „Tags“ herangezogen und das entsprechende „Tag“ wird in den entsprechenden patientenbezogenen Datensatz eingebunden, um diesen quasi mit einer Kennzeichnung für eine Archivierung zu versehen. Unter „Tag“ wird allgemein eine dem Datensatz hinzugefügte Zusatzinformation ver-
35 standen.

In vorteilhafter Weiterbildung werden die sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes zunächst

in Schlüsseldaten und sonstige sensitive Patientendaten eingeteilt und nachfolgend werden alle sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes anonymisiert, wodurch anonymisierte patientenbezogene Datensätze erzeugt werden. Jedoch werden mit Hilfe des Algorithmus nur aus den jeweiligen Schlüsseldaten eines jeden patientenbezogenen Datensatzes Prüfdaten generiert und in den jeweiligen patientenbezogenen Datensatz eingebunden. Die anonymisierten patientenbezogenen Datensätze mit den Prüfdaten werden nachfolgend in der Cloud-Computing-Architektur zur Verfügung gestellt. Im Rahmen einer Bearbeitung eines bestimmten patientenbezogenen Datensatzes werden an dem Client-Rechner, der an die Cloud-Computing-Architektur angebunden ist, Schlüsseldaten eines ausgewählten Patienten vorgegeben und mit Hilfe des Algorithmus werden aus diesen vorgegebenen Schlüsseldaten Abfragedaten generiert. Stimmen diese Abfragedaten des ausgewählten Patienten nicht mit den Prüfdaten des bestimmten patientenbezogenen Datensatzes überein, so wird infolge dessen die Sicherungsfunktion ausgelöst.

Diese Verfahrensvariante soll vor allem einen einfachen Umgang mit der hier vorgestellten Lösung erlauben. Dabei gilt es zu bedenken, dass die sensitiven Patientendaten mitunter sehr große Informationsmengen enthalten können, während bereits eine kleine Teilmenge in der Regel ausreichend ist, um den entsprechenden Patienten eindeutig zu identifizieren. Es ist also beispielsweise vorgesehen, dass ein Mediziner, der die medizinischen Daten seines Patienten abfragen möchte, von einer Anwendung auf seinem Rechner aufgefordert wird, den Namen und das Geburtsdatum seines Patienten in ein Eingabefenster einzutragen und dass diese Daten dann als Schlüsseldaten fungieren. Sonstige sensitive Patientendaten, die häufig ebenfalls in den patientenbezogenen Datensätzen enthalten sind, wie beispielsweise das Geschlecht des Patienten, dessen Anschrift, dessen Krankenversicherungsnummer usw., müssen dem Mediziner weder bekannt sein noch muss dieser jene Informationen über ein Eingabefenster eingeben. Die sonstigen sensitiven Patientendaten spielen also insbesondere bei der Identi-

fikation der patientenbezogenen Datensätze keine Rolle, werden aber ebenfalls anonymisiert, bevor die entsprechenden Datensätze in der Cloud-Computing-Architektur zur Verfügung gestellt werden.

5

Bevorzugt wird weiter eine Verfahrensvariante, bei der der Algorithmus durch eine Einweg-Hashfunktion, auch Hash-Algorithmus oder Streuwertfunktion genannt, gegeben ist. Zudem wird bevorzugt für die Anonymisierung der sensitiven Patientendaten und für die Generierung der Prüfdaten derselbe Algorithmus, insbesondere dieselbe Einweg-Hashfunktion, genutzt. Für die Kryptografie geeignete Einweg-Hashfunktionen sind dem Fachmann wohlbekannt, so dass sich ohne Weiteres eine Einweg-Hashfunktion mit günstigen Eigenschaften finden lässt. Von Vorteil sind hierbei insbesondere Einweg-Hashfunktionen vom Typ MD5, SHA1 oder SHA2.

Zweckmäßig ist zudem eine Verfahrensvariante, bei der eine Anzahl der anonymisierten patientenbezogenen Datensätze mit den Prüfdaten aus der Cloud-Computing-Architektur Anzeigedaten zur Anzeige am Client-Rechner enthalten. Ebenso ist eine Verfahrensvariante zweckmäßig, bei der eine Anzahl der patientenbezogenen Datensätze Bilddaten einer bilderzeugenen Modalität enthalten und bei der aus den Bilddaten einer dieser patientenbezogenen Datensätze in der Cloud-Computing-Architektur Anzeigedaten zur Anzeige am Client-Rechner erzeugt werden. Das bedeutet, dass beispielsweise Bilddaten, die an einem Computertomographen im Rahmen einer Untersuchung eines Patienten erzeugt werden, ebenfalls jedem Mediziner zur Verfügung stehen, der über einen Rechner Zugriff auf die über die Cloud-Computing-Architektur zur Verfügung gestellten gesammelten medizinischen Unterlagen seines Patienten hat. Dabei ist es insbesondere vorgesehen, dass die Bearbeitung der Bilddaten mit Hilfe von leistungsstarken Ressourcen innerhalb der Cloud-Computing-Architektur vorgenommen wird und dass lediglich Anzeigedaten an den Client-Rechner, also den Rechner des Mediziners, gesendet werden, die dann ohne eine weitere Bearbeitung am Anzeigegerät, also beispielsweise einem Moni-

tor, angezeigt werden. Es werden also quasi fertige Bilder zum Rechner des Mediziners geschickt, die dann lediglich bei ihm angezeigt werden. Die rechenintensive Aufbereitung der vom Computertomographen generierten Daten und insbesondere die Berechnung von 3D-Bildern erfolgt hingegen in der Cloud-Computing-Architektur. Der Datenumfang derartiger fertiger Bilder, die dann zum Rechner des Mediziners geschickt werden, ist zudem relativ gering. Während in der Cloud-Computing-Architektur beispielsweise ein sogenanntes „Volume Rendering“ vorgenommen wird, also zum Beispiel eine Bearbeitung der vom Computertomographen generierten Daten des gesamten untersuchten Volumens des Patienten, wird an den Rechner des Mediziners lediglich ein fertiges Bild einer einzelnen von ihm ausgewählten Ansicht auf das Volumen oder einer einzelnen Schnittdarstellung gesendet. Für eine Übertragung dieser Daten und somit für die Netzwerkanbindung des Rechners des Mediziners ist daher eine relativ geringe Bandbreite ausreichend.

Darüber hinaus wird eine Verfahrensvariante bevorzugt, bei der zunächst die Anzeigedaten und die Prüfdaten eines bestimmten anonymisierten patientenbezogenen Datensatzes am Client-Rechner zur Verfügung gestellt werden, bei der nachfolgend diese Prüfdaten mit den Abfragedaten verglichen werden und bei der die Sicherungsfunktion ausgelöst wird, wenn die Prüfdaten mit den Abfragedaten nicht übereinstimmen. Der Abgleich der Daten oder der Prüfprozess erfolgt somit bevorzugt zur Gänze lokal am Client-Rechner. Dieser Prüfprozess wird dabei bevorzugt durch einen separate und damit von der Bearbeitung der anonymisierten patientenbezogenen Datensätze gänzlich getrennte Anwendung umgesetzt, so dass hierdurch die gewünschte strikte Trennung der anonymisierten patientenbezogenen Datensätze von den Klardaten gewährleistet wird.

Außerdem ist eine Verfahrensvariante von Vorteil, bei der die Prüfdaten in die Anzeigedaten grafisch und weiter bevorzugt nach Art eines 2D-Barcodes eingebunden werden. Wird also beispielsweise über die Cloud-Computing-Architektur ein Röntgen-

Bild vom Patienten zur Verfügung gestellt, welches am Monitor des Rechners des Mediziners lediglich angezeigt wird, so befindet sich beispielsweise in einem vorgegebenen Bereich des angezeigten Bildes, zum Beispiel in der rechten oberen Ecke, die Abbildung eines Strich-Codes oder eines QR-Codes, die die anonymisierten sensitiven Patientendaten und insbesondere die Schlüsseldaten repräsentiert. Ein in diesem Fall geeigneter Abfrageprozess, dieser ist Teil des Verfahrens, ist dann beispielsweise wie folgt gestaltet. Zunächst gibt der Mediziner den Namen und das Geburtsdatum seines Patienten in ein Eingabefenster ein, woraufhin mittels einer gegebenen Einweg-Hashfunktion auf der Basis des Namens und des Geburtsdatums ein QR-Code generiert wird. Zusätzlich wird mit Hilfe einer zweiten Einweg-Hashfunktion ein Zahlencode generiert. In der Cloud-Computing-Architektur wird daraufhin eine Datei aufgerufen, in der derselbe Zahlencode als „Tag“ eingebunden ist. Die Bilddaten aus dieser Datei werden daraufhin bearbeitet, so dass hierdurch ein Satz Anzeigedaten generiert wird. Die Anzeigedaten werden dann an den Rechner des Mediziners gesendet, wobei diese Anzeigedaten ebenfalls einen QR-Code enthalten. Daraufhin wird der Prüfprozess gestartet, bei dem der QR-Code aus der Anzeige und der am Rechner des Mediziners generierte QR-Code vorzugsweise auf Softwarebasis quasi optisch miteinander verglichen werden. Stimmen die beiden QR-Codes überein, so werden die Anzeigedaten als Bild am Monitor des Rechners des Mediziners angezeigt. Dieses Bild wird dann bevorzugt im Bereich des angezeigten QR-Codes durch ein zweites Bild überlagert, in welchem die Klardaten, die durch den QR-Code repräsentiert werden, also der Name und das Geburtsdatum des Patienten, angezeigt werden. Der Mediziner sieht somit nicht ein Röntgenbild in dessen oberer rechter Ecke ein QR-Code abgebildet ist, sondern ein Röntgenbild, in dessen oberer rechter Ecke der Name und das Geburtsdatum des Patienten zu sehen und zu lesen sind. Stimmen die beiden QR-Codes hingegen nicht überein, so wird die Sicherungsfunktion ausgelöst und es wird beispielsweise eine Fehlermeldung angezeigt.

Vorteilhaft ist zudem eine Verfahrensvariante, bei der eine Anzeige der Anzeigedaten unterbunden wird, wenn die Sicherungsfunktion ausgelöst wird. Stimmen also die Prüfdaten und die Abfragedaten nicht überein, so bekommt der Mediziner die Anzeigedaten nicht angezeigt und somit nicht zu sehen. Wird also beispielsweise ein Röntgenbild eines Patienten in der Cloud-Computing-Architektur quasi in einer Patientenakte eines anderen Patienten abgelegt und versucht nun ein Mediziner die medizinischen Unterlagen in dieser Patientenakte zu sehen, so wird dieser beim Versuch, sich das Röntgenbild anzusehen, eine Warnmeldung erhalten, dass das Röntgenbild kein Röntgenbild seines Patienten ist und das Röntgenbild wird nicht angezeigt.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand einer schematischen Zeichnung näher erläutert. Darin zeigen:

FIG 1 in einer Blockschaltdarstellung ein Verfahren zur Bearbeitung von patientenbezogenen Datensätzen.

Die nachfolgend exemplarisch beschriebene Verfahrensvariante erlaubt es ein Archiv für medizinische Daten außerhalb des untermittelbaren Kontrollbereichs einer medizinischen Einrichtung, hier einem Krankenhaus, anzusiedeln. Dieses Archiv ist dabei auf mehrere PACS-Server (Picture Archiving and Communication System) verteilt, die Teil einer Cloud-Computing-Architektur 2 sind.

Soll nun ein Patient beispielsweise mit Hilfe eines Computertomographen 4 im Krankenhaus untersucht werden, so werden im Vorfeld der Untersuchung während eines Eingabe-Prozessschrittes 6 zunächst einmal einige sensitive Patientendaten, wie beispielsweise der Name des Patienten und dessen Geburtsdatum, in einem Speicher des Computertomographen 4 hinterlegt. Anschließend erfolgt die eigentliche Untersuchung des Patienten, bei der mittels des Computertomographen 4 während eines Scan-Prozessschrittes 8 Rohdaten generiert werden. Ist dieser Scan-Prozessschritt 8 abgeschlossen, so wird aus den Rohdaten

ein patientenbezogener Datensatz erstellt, in welchen im Rahmen eines Einbettungs-Prozessschrittes 10 die sensitiven Patientendaten, die im Eingabe-Prozessschritt 6 eingegeben wurden, eingebunden werden. Diese sensitiven Patientendaten werden darüber hinaus durch weitere sensitive Patientendaten ergänzt, welche die am Computertomographen 4 durchgeführte Untersuchung charakterisieren und eindeutig kennzeichnen. Dies sind beispielsweise Datum und Uhrzeit der Untersuchung, der Untersuchungsmodus, die Strahlungs-dosis der der Patient ausgesetzt war usw.. Dieser patientenbezogene Datensatz wird so-
dann an eine Serverstation 12 innerhalb des unmittelbaren Kontrollbereichs des Krankenhauses übertragen.

In der Serverstation 12 werden die Rohdaten des patientenbezogenen Datensatzes weiterverarbeitet und während eines Bild-Prozessschrittes 14 in Bilddaten, genauer in sogenannte Transversalschnitte, umgewandelt. Der so bearbeitete patientenbezogene Datensatz wird nachfolgend als Kopie in der Serverstation 12 hinterlegt und zusätzlich für eine Speicherung im Archiv für medizinische Daten außerhalb des unmittelbaren Kontrollbereichs des Krankenhauses, also in der Cloud-Computing-Architektur 2, aufbereitet.

Dazu wird in den patientenbezogenen Datensatz ein zusätzliches „Tag“ zur Kennzeichnung eingebunden, welches eine Ziffernfolge oder Zeichenfolge als Prüfdaten enthält. Bei diesen Prüfdaten handelt es sich um anonymisierte Schlüsseldaten, wobei die Schlüsseldaten wiederum den patientenbezogenen Datensatz eindeutig dem Patienten zuordnen. Im Ausführungsbeispiel werden im Rahmen eines Auswahl-Prozessschrittes 16 aus den sensitiven Patientendaten der Name des Patienten und dessen Geburtsdatum als Schlüsseldaten ausgewählt. Nachfolgend werden aus diesen Schlüsseldaten mittels einer Einweg-Hash-funktion die Prüfdaten, hier die Ziffern- oder Zeichenabfolge, generiert und mit Hilfe des zusätzlichen „Tags“ zur Kennzeichnung des patientenbezogenen Datensatzes in diesen eingebunden. Zusätzlich werden in einem Anonymisierungs-Prozessschritt 20 alle in dem patientenbezogenen Datensatz enthalte-

nen sensitiven Patientendaten mit Hilfe derselben Einweg-Hashfunktion anonymisiert und durch Ziffern- oder Zeichenabfolgen als Platzhalter ersetzt. Darüber hinaus werden die Schlüsseldaten als Prüfdaten in Form eines QR-Codes in jeden
5 Transversalschnitt eingebaut, so dass dieser QR-Code bei der Darstellung eines entsprechenden Transversalschnittes an einem Monitor stets am rechten oberen Bildrand abgebildet wird. Der entsprechende QR-Code wird dabei mittels weiteren Hash-Algorithmus, eines 2D-Barcode-Hash-Algorithmus, aus den
10 Schlüsseldaten generiert.

Der auf diese Weise anonymisierte patientenbezogene Datensatz wird sodann aus dem unmittelbaren Kontrollbereich des Krankenhauses in die Cloud-Computing-Architektur 2 abgegeben und
15 dort im Zuge eines Ablage-Prozessschrittes 22 im Archiv für medizinische Unterlagen gespeichert. Sofern dies der erste anonymisierte patientenbezogene Datensatz des Patienten ist wird zunächst im Archiv eine neue Patientenakte angelegt, welche durch die Prüfdaten, also die entsprechende Ziffern- oder Zeichenabfolge, gekennzeichnet ist. Anschließend wird
20 der anonymisierte patientenbezogene Datensatz in die neu angelegte Patientenakte eingepflegt. Existiert bereits eine Patientenakte mit den entsprechenden Prüfdaten, so entfällt das Anlegen einer neuen Patientenakte und der anonymisierte patientenbezogene Datensatz wird der Patientenakte mit den Prüf-
25 daten des anonymisierten patientenbezogenen Datensatzes zugeordnet.

Wird nun ein Mediziner vom Patienten beauftragt, die am Computertomographen 4 im Krankenhaus vorgenommene Untersuchung
30 diagnostisch auszuwerten, so hat dieser die Möglichkeit, über einen Clientrechner 24, der an die Cloud-Computing-Architektur 2 angebunden ist, auf das Archiv für medizinische Unterlagen zuzugreifen. Hierzu startet der Mediziner eine lokal am
35 Clientrechner 24 zur Verfügung stehende Anwendung, durch die er aufgefordert wird, die Schlüsseldaten des Patienten, also dessen Name und dessen Geburtsdatum, in ein Eingabefenster am Clientrechner 24 einzugeben. Mit Hilfe derselben Einweg-

Hashfunktion, mit der die sensitiven Patientendaten des patientenbezogenen Datensatzes in der Serverstation 12 des Krankenhauses anonymisiert wurden, werden im Rahmen eines Anfrage-Prozessschrittes 26 am Clientrechner 24 durch die Anwendung Abfragedaten, also wiederum eine Ziffern- oder Zeichenabfolge, generiert. Daraufhin wird im Archiv für medizinische Unterlagen in der Cloud-Computing-Architektur 2 nach Datensätzen gesucht, deren Prüfdaten mit den Abfragedaten übereinstimmen bzw. deren Ziffern- oder Zeichenabfolge mit der am Clientrechner 24 erzeugten Ziffern- oder Zeichenabfolge übereinstimmt. Werden entsprechende Datensätze gefunden, so wird der Mediziner aufgefordert aus einer Auswahl eine Art der Darstellung auszuwählen, also z.B. eine Schnittdarstellung mit speziell gewählter Schnittebene oder eine 3D-Darstellung einer gewählten Körperregion. Daraufhin wird der gefundene anonymisierte patientenbezogene Datensatz im Rahmen eines Bearbeitungs-Prozessschrittes 28 in der Cloud-Computing-Architektur 2 aufbereitet, wodurch Anzeigedaten zur Anzeige an einem Monitor generiert werden. Bei einer solchen Aufbereitung handelt es sich beispielsweise um eine sogenannte multiplanare Reformatierung (MRT), auch multiplanare Rekonstruktion genannt, bei der aus den Transversalschnitten Schnittdarstellungen mit beliebig gewählter Schnittebene berechnet werden, um eine Bildverarbeitung nach dem MIP-Prinzip (Maximum Intensity Protection) oder auch um ein sogenanntes Raycasting-Verfahren. In jedem Fall wird der QR-Code, der in jedem Transversalschnitt enthalten ist, auch in die Anzeigedaten eingebettet.

Die Anzeigedaten werden dann an den Clientrechner 24 übertragen und dort im Zuge eines Abgleich-Prozessschrittes 30 gegengeprüft. Zu diesem Zwecke werden die vom Mediziner am Clientrechner 24 eingegebenen Schlüsseldaten mit Hilfe des zuvor genannten 2D-Barcode-Hash-Algorithmus in einen QR-Code umgewandelt und der so generierte QR-Code wird mit dem QR-Code in den Anzeigedaten aus der Cloud-Computing-Architektur 2 verglichen. Stimmen die beiden QR-Codes nicht überein so wird eine Sicherungsfunktion ausgelöst, infolgedessen die An-

zeigedaten vom Clientrechner 24 verworfen werden und infolgedessen am Monitor des Clientrechners 24 eine Fehlerbenachrichtigung erscheint, die den Mediziner darauf aufmerksam macht, dass die Anzeigedaten einem unbekannten Patienten zugeordnet sind. Stimmen die QR-Codes hingegen überein so werden die Anzeigedaten im Rahmen eines Freigabe-Prozessschrittes 32 freigegeben und als Bild am Monitor des Clientrechners 24 dargestellt. Mit Hilfe der vom Mediziner lokal am Clientrechner 24 gestarteten Anwendung wird außerdem im Rahmen eines Überlapp-Prozessschrittes 34 ein zusätzliches Bild erzeugt, welches über das auf den Anzeigedaten basierende Bild gelegt wird. Dadurch sieht der Mediziner am Monitor des Clientrechners 24 nicht das gewünschte Röntgenbild, in welchem oben rechts der QR-Code abgebildet wird, sondern das gewünschte Röntgenbild, in dem oben rechts die Schlüsseldaten als Klardaten abgebildet sind, also in dem oben rechts der Name und das Geburtsdatum des Patienten zu lesen sind.

Die Erfindung ist nicht auf das vorstehend beschriebene Ausführungsbeispiel beschränkt. Vielmehr können auch andere Varianten der Erfindung von dem Fachmann hieraus abgeleitet werden, ohne den Gegenstand der Erfindung zu verlassen. Insbesondere sind ferner alle im Zusammenhang mit dem Ausführungsbeispiel beschriebenen Einzelmerkmale auch auf andere Weise miteinander kombinierbar, ohne den Gegenstand der Erfindung zu verlassen.

Patentansprüche

1. Verfahren zur Bearbeitung von patientenbezogenen Datensätzen, die jeweils medizinische Daten und sensitive Patientendaten als Klardaten umfassen,

- bei dem die sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes anonymisiert werden (20), wodurch anonymisierte patientenbezogene Datensätze erzeugt werden,

- bei dem mit Hilfe eines Algorithmus aus den jeweiligen sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes Prüfdaten generiert und in dem jeweiligen patientenbezogenen Datensatz eingebunden werden (18),

- bei dem die anonymisierten patientenbezogenen Datensätze mit den Prüfdaten in einer Cloud-Computing-Architektur (2) zur Verfügung gestellt werden (22),

- bei dem an einem Clientrechner (24), der an die Cloud-Computing-Architektur (2) angebunden ist, im Rahmen einer Bearbeitung eines bestimmten patientenbezogenen Datensatzes sensitive Patientendaten eines ausgewählten Patienten vorgegeben werden und bei dem mit Hilfe des Algorithmus aus diesen vorgegeben sensitiven Patientendaten Abfragedaten generiert werden (26) und

- bei dem eine Sicherungsfunktion ausgelöst wird, wenn die Prüfdaten des bestimmten patientenbezogenen Datensatzes nicht mit den Abfragedaten des ausgewählten Patienten übereinstimmen.

2. Verfahren nach Anspruch 1,

- bei dem die sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes in Schlüsseldaten und sonstige sensitive Patientendaten eingeteilt werden (16),

- bei dem alle sensitiven Patientendaten eines jeden patientenbezogenen Datensatzes anonymisiert werden (20), wodurch anonymisierte patientenbezogene Datensätze erzeugt werden,

- bei dem jedoch mit Hilfe des Algorithmus nur aus den jeweiligen Schlüsseldaten eines jeden patientenbezogenen

Datensatzes Prüfdaten generiert und in dem jeweiligen patientenbezogenen Datensatz eingebunden werden (18),

- bei dem die anonymisierten patientenbezogenen Datensätze mit den Prüfdaten in einer Cloud-Computing-Architektur (2) zur Verfügung gestellt werden,
- bei dem an einem Clientrechner (24), der an die Cloud-Computing-Architektur (2) angebunden ist, im Rahmen einer Bearbeitung eines bestimmten patientenbezogenen Datensatzes Schlüsseldaten eines ausgewählten Patienten vorgegeben werden und bei dem mit Hilfe des Algorithmus aus diesen vorgegeben Schlüsseldaten Abfragedaten generiert werden (26) und
- bei dem eine Sicherungsfunktion ausgelöst wird, wenn die Prüfdaten des bestimmten patientenbezogenen Datensatzes nicht mit den Abfragedaten des ausgewählten Patienten übereinstimmen.

3. Verfahren nach Anspruch 1 oder 2, bei dem der Algorithmus durch eine Einweg-Hashfunktion gegeben ist.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem eine Anzahl der anonymisierten patientenbezogenen Datensätze mit den Prüfdaten aus der Cloud-Computing-Architektur (2) Anzeigedaten zur Anzeige am Clientrechner (24) enthalten.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem eine Anzahl der patientenbezogenen Datensätze Bilddaten einer bilderzeugenden Modalität (4) enthalten und bei dem aus den Bilddaten einer dieser patientenbezogenen Datensätze in der Cloud-Computing-Architektur (2) Anzeigedaten zur Anzeige am Clientrechner (24) erzeugt werden (28).

6. Verfahren nach einem der Ansprüche 1 bis 3 und 4 oder 5, bei dem zunächst die Anzeigedaten und die Prüfdaten eines bestimmten anonymisierten patientenbezogenen Datensatzes am Clientrechner (24) zur Verfügung gestellt werden, bei dem

nachfolgend diese Prüfdaten mit den Abfragedaten verglichen werden (30) und bei dem die Sicherungsfunktion ausgelöst wird, wenn die Prüfdaten mit den Abfragedaten nicht übereinstimmen.

5

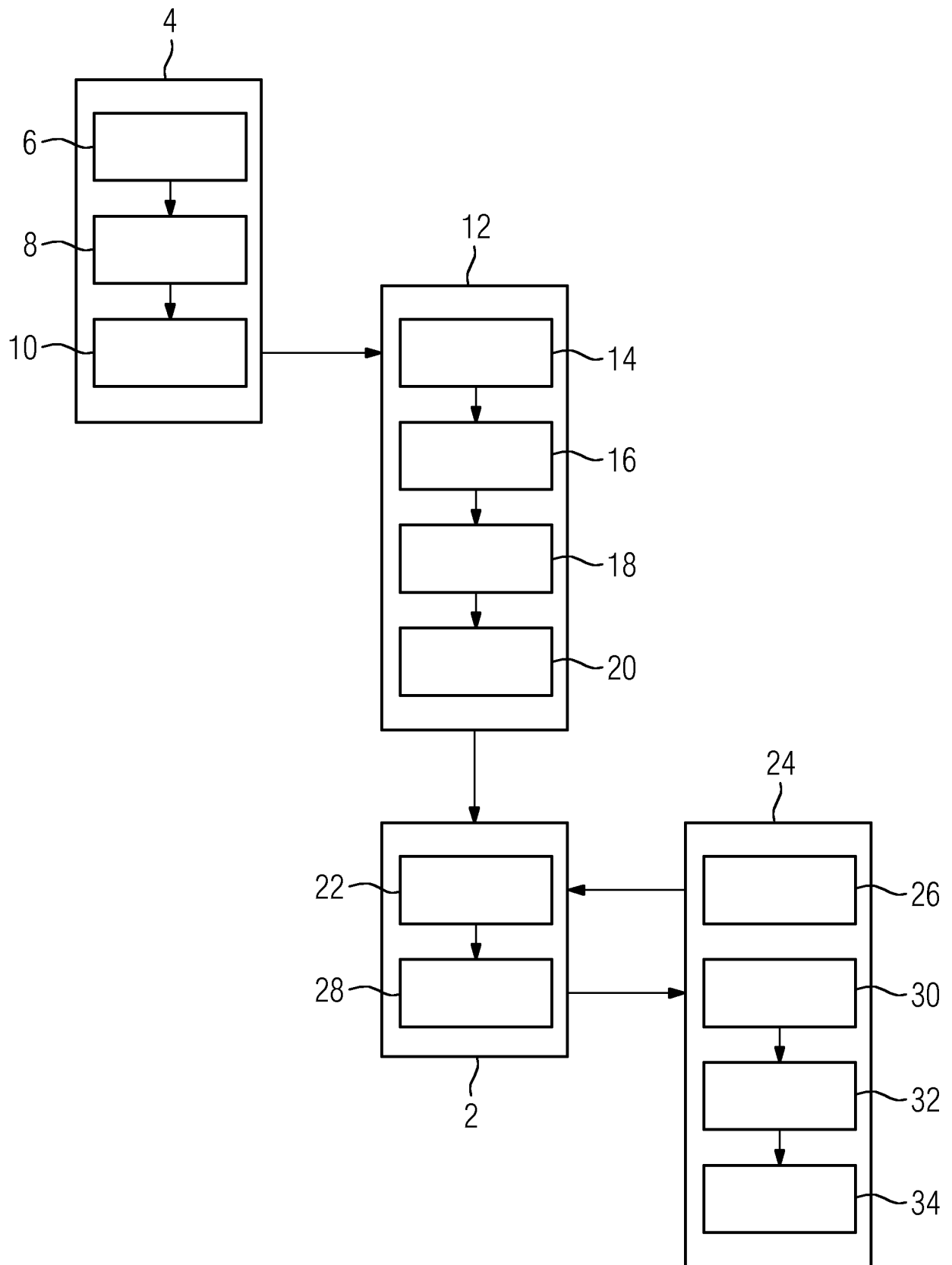
7. Verfahren nach einem der Ansprüche 1 bis 6 und 4 oder 5, bei dem die Prüfdaten in die Anzeigedaten graphisch eingebunden sind.

10

8. Verfahren nach Anspruch 7, bei dem die Prüfdaten als 2D-Barcode in die Anzeigedaten eingebunden sind.

15

9. Verfahren nach einem der Ansprüche 1 bis 8 und 4 oder 5, bei dem eine Anzeige der Anzeigedaten unterbunden wird, wenn die Sicherungsfunktion ausgelöst wird.



INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2012/074334

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q10/10

ADD.

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)

G06Q

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 practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
L	<p>EP0: "Mitteilung des Europäischen Patentamts vom 1. Oktober 2007 über Geschäftsmethoden = Notice from the European Patent Office dated 1 October 2007 concerning business methods = Communiqué de l'Office européen des brevets, en date du 1er octobre 2007, concernant les méthodes dans le domaine des activités",</p> <p>JOURNAL OFFICIEL DE L'OFFICE EUROPEEN DES BREVETS.OFFICIAL JOURNAL OF THE EUROPEAN PATENT OFFICE.AMTSBLATT DES EUROPAEISCHEN PATENTAMTS, OEB, MUNCHEN, DE, vol. 30, no. 11, 1 November 2007 (2007-11-01), pages 592-593, XP007905525, ISSN: 0170-9291</p> <p>Der gemäß Regel 33(3) PCT unter angemessener Berücksichtigung der Beschreibung und der Zeichnungen</p>	1-9



Further documents are listed in the continuation of Box C.



See patent family 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 application or patent 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

22 February 2013

Date of mailing of the international search report

01/03/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Moltenbrey, Michael

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2012/074334

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	<p>betrachtete Anspruchsgegenstand bezieht sich auf Verfahren aus der Liste von Gegenständen und Tätigkeiten, die nach Regel 39 PCT von der Patentierbarkeit ausgeschlossen sind. Die Informationstechnologie, die als Vehikel zur Ausführung der genannten Verfahren eingesetzt wird, ist konventioneller Art. Ihre Verwendung zur Ausführung nichttechnischer Verfahren gehört zum allgemeinen Fachwissen, und sie war am Anmeldetag der vorliegenden Anmeldung jedermann ohne Weiteres zugänglich. Die Angabe von Unterlagen erübrigt sich somit.</p> <p>-----</p>	

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

INV. G06Q10/10

ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

G06Q

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
L	<p>EP0: "Mitteilung des Europäischen Patentamts vom 1. Oktober 2007 über Geschäftsmethoden = Notice from the European Patent Office dated 1 October 2007 concerning business methods = Communiqué de l'Office européen des brevets, en date du 1er octobre 2007, concernant les méthodes dans le domaine des activités",</p> <p>JOURNAL OFFICIEL DE L'OFFICE EUROPEEN DES BREVETS.OFFICIAL JOURNAL OF THE EUROPEAN PATENT OFFICE.AMTSBLATT DES EUROPÄISCHEN PATENTAMTS, OEB, MUNCHEN, DE, Bd. 30, Nr. 11, 1. November 2007 (2007-11-01), Seiten 592-593, XP007905525, ISSN: 0170-9291</p> <p>Der gemäß Regel 33(3) PCT unter angemessener Berücksichtigung der Beschreibung und der Zeichnungen</p>	1-9



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

22. Februar 2013

Absendedatum des internationalen Recherchenberichts

01/03/2013

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Moltenbrey, Michael

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
	<p>betrachtete Anspruchsgegenstand bezieht sich auf Verfahren aus der Liste von Gegenständen und Tätigkeiten, die nach Regel 39 PCT von der Patentierbarkeit ausgeschlossen sind. Die Informationstechnologie, die als Vehikel zur Ausführung der genannten Verfahren eingesetzt wird, ist konventioneller Art. Ihre Verwendung zur Ausführung nichttechnischer Verfahren gehört zum allgemeinen Fachwissen, und sie war am Anmeldetag der vorliegenden Anmeldung jedermann ohne Weiteres zugänglich. Die Angabe von Unterlagen erübrigt sich somit.</p> <p>-----</p>	