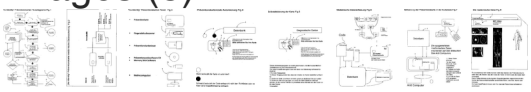
"No-Identity" Prevention card

Abstract

Die "No-Identity" Präventionskarte sichert dem Nutzer seine persönliche Datensicherheit in der Gesundheitsprävention. Daten können nur ohne Identität abgespeichert werden und eine Zuordnung der Daten zu einer Person ist nur im Beisein der Person befristet möglich.

Images (8)



Classifications

G06K19/0718 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips at least one of the integrated circuit chips comprising a sensor or an interface to a sensor the sensor being of the biometric kind, e.g. fingerprint sensors

DE102009050291A1

DE Application

Other languages English Inventor Peter Roehr Original Assignee Röhr, Peter, Dipl.-Ing. Priority date 2009-10-15

Family: DE (1)

Date	App/Pub Number	Status
2009-10-15	DE200910050291	Withdrawn
2011-04-21	DE102009050291A1	Application

Info Legal events Similar documents Priority and Related Applications External links EspacenetGlobal DossierDPMADiscuss

Description

- [0001] Die Erfindung bezieht sich auf eine elektronische „No-Identity" Präventionskarte nach dem Oberbegriff der Patentansprüche 1–10
- Hintergrund der Erfindung:
- [0002] Im Dienst der Wissenschaft und der sich daraus immer besseren medizinischen Versorgung wird es in der Zukunft notwendig sein einen

schnellen Zugriff zu medizinischen Daten zu erhalten. Dabei gibt es zwei entscheidende Faktoren bester Nutzung:

- 1. Die Wissenschaft und Forschung benötigt medizinische Daten und deren Auswertung, um Systeme zu analysieren und auf breiter Basis neue Behandlungskonzepte und präventive Maßnahmen zu entwickeln. Unsere Bevölkerung speziell in den Industrieländern wird immer älter so geht die durchschnittliche Lebenserwartung schon in den nächsten Jahren in Deutschland allein auf 86 Jahren bei Frauen und 81 Jahren bei Männern. Neue Krankheiten entstehen meist erst im hohen Alter die anspruchsvolle und neue Wege der medizinischen Versorgung erfordern.
- 2. Der Nutzer, der Mensch braucht beste medizinische Betreuung auf der Basis seiner medizinischen Daten. Je genauer, ganzheitlicher diese Daten sind je besser ist die Chance einer professionellen und Erfolg versprechender Behandlung. Dabei sind Kosten sicherlich ein wesentlicher Faktor und es gilt effektive Systeme zu schaffen.

•

- [0003] Die Basis wäre ein 100 Prozent sicherer Datenfluss. Dieses Thema ist heute in vielen Ländern unter deren bestehenden Gesundheitssystemen diskutiert und zerredet. Die Einführung einer elektronischen Gesundheitskarte wäre mit Blick auf telematische Infrastrukturen innerhalb von Klinikkonzernen, von Krankenhäusern, Klinikverbünden von enormem Vorteil. Heute stellen sich die Anbieter der Gesundheitskarte das wie folgt vor: Der Schlüssel die e-Karte wird von der Krankenkasse erzeugt und an den Kartenhersteller ausgeliefert. Er wird zudem für den Fall des Verlustes der Karte bei einem so genannten Treuhänderdienst hinterlegt. An diesen drei Stellen – Kassen, Kartenhersteller und Treuhänderdienst – finden sich Angriffspunkte für Interessenten an den Daten. Täglich gibt es in den Medien Berichte wie diese Daten veruntreut werden könnten. Somit könnte der Nutzer zum gläsernen und vor allem staatlich steuerbaren Menschen werden. Daten, die zunächst für Rechnungszwecke gespeichert wurden könnten zur Bekämpfung von Kriminalität herangezogen werden. Der Arbeitgeber könnte Kenntnis über die Gesundheit seiner Mitarbeiter erhalten oder erhält Informationen über die Erkrankungen eines Bewerbers, die potenziell dessen Leistungsfähigkeit einschränkt. Der Mensch, der Bürger will nicht Opfer werden eines unkontrollierten Zugriffs seiner sehr persönlichen und intimen medizinischen Daten ohne seine ausdrückliche kontrollierte Zustimmung.
- [0004] Das Grundrecht auf die Datenhoheit über persönliche Gesundheitsdaten des Patienten ist unter den heutigen Gesichtspunkten subjektiv sowohl objektiv in erheblicher Gefahr. Durch zentrale Datenspeicherung ist der Datenschutz stark gefährdet. Die Ausspähung

der zentralen Datenbank ist für Dritte/Unbefugte) ist von größtem wirtschaftlichem Interesse. Die Möglichkeit des Zugangs zur zentralen Datenbank für die Gesundheitsbürokratie und für viele Gesundheitsberufe erhöht die Datenunsicherheit.

- [0005] Vor diesem Hintergrund gilt es ein eigenständiges System für die Gesundheitsprävention zu entwickeln und zu erfinden, das sowohl subjektiv als auch objektiv für den Menschen 100% sicher ist. Die ”No-Identity” Präventionskarte wird diesem Anspruch gerecht. Medizinische Daten werden ohne Identität erfasst und gespeichert. Konsequent können medizinische Daten niemals ohne die persönliche Anwesenheit des betroffenen Menschen zugeordnet werden. Die Datenspeicherung erfolgt über einen persönlichen Code der auf einer elektronischen Präventionskarte abgespeichert ist. Es gibt kein Trustcenter, die Karte wird weder von der Versicherung noch von einem Dritten bestimmt. Der Nutzer codiert seine Karte ohne Internet an seinem Heimcomputer. Der persönliche Code unaktiviert wird auf den Chip geschrieben. Die Autorisation von einer zentralen Datenstelle des Codes erfolgt später bei der Aktivierung des Codes mit Fingerabdruck und Geheimzahl, wie im Einzelnen wird nachfolgend beschrieben. Zum Verständnis- des Nutzens dieser Erfindung gilt es zu verstehen, das diese Anwendung nur in der Gesundheitsprävention zunächst denkbar ist als ein losgelöstes eigenständiges privates System. Dabei können auf Daten nicht in einer Notsituation zugegriffen werden. Ist der Mensch nicht bei Bewusstsein und nicht persönlich in der Lage seine Präventionskarte zu aktivieren so wird es nicht möglich sein an die Daten zu kommen. Verliert er die Karte, so kann er nur in seinem Privatbereich eine neue Karte selbst codieren sofern er den ursprünglichen Code privat hinterlegt hat. Ist auch der Code privat verloren, vergessen so sind die Daten für immer verloren. Die Hinterlegung des Codes bei einem Trustcenter ist nicht vorgesehen in dieser Erfindung jedoch theoretisch möglich. Im Präventionsgesundheitssystem ist alles auf freiwilliger und privater Nutzung, die Menschen sind genügend gesund. Ein Transfer von Daten und die Öffnung der Identität sind innerhalb dieser Erfindung ausgeschlossen. Die Nutzung der medizinischen Daten ist ohne Identitätszuweisung für die Wissenschaft und über die Telemedizin zur internationalen Auswertung möglich.
- Kurze Beschreibung der Erfindung:
- [0006] Es galt eine 100% sichere medizinische Datenkarte zu erfinden. Einen Schlüssel der nicht gehackt werden kann. Es war notwendig in den Gedanken alle heutigen Fehlstellen wie Trustcenter und Dritte auszuschließen. Somit erhält die Erfindung den Namen ”No-Identity” Präventionskarte. Wie der Name schon erkennen lässt können medizinische Daten in diesem Fall nur ohne Identität abgespeichert werden. Dadurch dass die Daten keine Identität haben muss nicht unbedingt eine komplizierte Verschlüsselung der Daten vorgenommen

werden. Die Daten können frei abgespeichert werden auf einen zentralen Datenspeicher. Sollte dieser Datenspeicher gehackt werden so gibt es da zwar medizinische Daten die jedoch keiner bestimmten Person jemals zugeordnet werden können. Zum weiteren Verständnis ist es notwendig das es sich hier nur um ein beschränktes Einsatzgebiet handelt die Gesundheitsprävention. Also um Menschen die noch gesund sind oder zumindest genügend gesund sind. Es handelt sich um eine freiwillige und eigenverantwortliche Basis. Kein Mensch kann gezwungen werden etwas für seine Gesundheit zu tun, wenn er das nicht ausdrücklich selber möchte. Auf dieser Basis werden nun medizinische Daten ohne Identität abgespeichert zum Nutzen der Wissenschaft und zum Nutzen des betroffenen Menschen. Eine normale blanke Chip-Karte, eine Software-CD, ein Kartenlesegerät und ein Fingerabdruckleser werden vom Nutzer bezogen. Der Versand erfolgt an die private Adresse. Der Nutzer öffnet das zugesandte Paket und schließt das Kartenlesegerät an den Computer an. Die gelieferte Software-CD wird in den Computer geladen. Direkt öffnet sich ein Programm, es wird nicht auf den Computer geladen und fordert den Nutzer auf zunächst das Internet abzuschalten. Danach erfolgt die Bitte die gelieferte Chip-Karte in das Kartenlesegerät einzuschieben. Der Nutzer wird informiert Chip-Karte eingerichtet, Internet ist ausgeschaltet. Die Software wird dies ebenfalls noch einmal prüfen. Danach erfolgt die Aufforderung einen 17 Stellen Code einzutippen mit 13 beliebigen Dezimalzahlen und 4 Buchstaben des Alphabets an beliebiger Stelle. Sind die Zahlen vollständig und korrekt eingegeben wird der Code auf den Chip der Karte unaktiviert verschlüsselt aufgespielt. Sollte an dieser Stelle die Karte verloren gehen so hat sie keinerlei Informationen nur einen Code der verkryptet ist und auch zu niemand zugeordnet werden kann. Der Nutzer nimmt nun die Karte mit verschlüsseltem Code in seinen Besitz und kann nun zur Präventionsklinik zu einer diagnostischen Untersuchung gehen. Um die Diagnosedaten abspeichern zu können, bedarf es einer Aktivierung der Präventionskarte. Der Nutzer steckt vor der Diagnose die Karte in eine Lesestelle zur Aktivierung. Ein Geheimcode und Fingerabdruck sind nun notwendig, um den verkrypten Code auf der Karte über einen Timer-Chip zu aktivieren. Mit anderen Worten die Karte kann nur für maximal zwei Stunden aktiv bleiben und desaktiviert sich danach selber über den Timer-Chip. Der Nutzer hat nun eine aktivierte Karte in der Hand und begibt sich zu den diagnostischen Untersuchungen. Jede medizinische Untersuchung führt zu medizinischen Daten die nun mit Hilfe der aktivierten Präventionskarte codiert auf einer zentralen Datenbank abgespeichert werden kann. Keine der medizinischen Daten hat auch nur eine persönliche Identitätsinformation außerdem eigenen angelegten 17 Stellen Code. Mehrere Untersuchungen folgen alle Daten sind unter demselben Code abgespeichert. Nun haben autorisierte

Stellen wie Kliniken, die Wissenschaft autorisierten Zugang zu den gespeicherten Daten und eine Auswertung kann bei einem Betreiber wo auch immer ausgewertet werden. Die Ergebnisse werden dann wieder auf der Datenbank gespeichert. Der Nutzer hat es nun ermöglicht dass seine medizinischen Dauten seiner Diagnose abgespeichert sind. Nach der vollen Auswertung geht der Nutzer zu einem Arzt seines Vertrauens und in seinem Beisein wird er gebeten die Verbindung mit Hilfe seiner Präventionskarte herzustellen. Der Nutzer nimmt die Karte und führt sie in das Lesegerät des Arztes, wiederum erfolgt der Aufforderung eine 4 Stellen Geheimzahl einzugeben und den Fingerabdruck. Dadurch wird der Code aktiviert und die gespeicherten medizinischen Daten können im Beisein des Nutzers zugeordnet werden. Der Arzt hat die komplette diagnostische Auswertung auf seinem Bildschirm allerdings auch hier ohne Namen und Identität. Der Arzt weiß nur dass die Daten zu dem Nutzer gehören da er in dem Arztraum präsent ist. Sollte der Nutzer im Anschluss die Karte vergessen so sorgt der Timer-Chip für eine automatische Desaktivierung der Karte. Nachdem die Besprechung mit dem Arzt abgeschlossen ist verschwinden die Daten beim herausziehen der Karte automatisch von dem Bildschirm. In der Prävention ist diese Erfindung außergewöhnlich nützlich da sie die Basis schafft für einen wirtschaftlichen effektiven Ansatz in der Präventionsmedizin. Genetische Test und andere kritische Untersuchungen haben nun eine solide Basis auf der Basis eine 100% Datensicherheit sowohl subjektiv als auch objektiv für den Nutzer.

- Beschreibung der Anlagen:
- [0007] Weiter Details neben der Beschreibung der Erfindung findet man in den beiliegenden Zeichnungen:
- [0008] 1 Es handelt sich um ein Flussdiagramm der logistischen Abfolge des „No-Identity” Präventionskartensystems
- [0009] 2 Es handelt sich um die Darstellung der zwei Ebenen Identität und keine Identität
- [0010] 3 Es wird das Heimpaket der Präventionskarte gezeigt mit den Komponenten, Fingerabdruckscanner, die elektronische Datenkarte, Das Kartenlesegerät und die Software CD.
- [0011] 4 Zeigt schematisch die Autorisierung des Präventionskartencodes
- [0012] 5 Demonstriert die Selbstaktivierung des Präventionskartencodes mit dem Scannen des Fingerabdruckes und der Eingabe einer 4 Stellen Geheimzahl.
- [0013] 6 Hier wird die medizinische Datenerfassung und Datenfluss zur Speicherung in der Datenbank mit der aktivierten Präventionskarte gezeigt.
- [0014] 7 Es erfolgt die Aktivierung des Codes der Präventionskarte in der Arztpraxis und der Datenfluss von der Datenbank zu dem Bildschirm des gegenübersitzenden Arztes.
- [0015] 8 Die medizinische Datei im aktivierten Zustand zeigt den markierten

Code und symbolisch zum Zeitpunkt der Aktivierung wird die Präventionskarte unter dem Code gezeigt. Nun weiß der Arzt bestimmt die Daten gehören der gegenüberliegenden Person.

- [0016] 9 Die medizinische Datei im desaktivierten Zustand zeigt nur den markierten Code. Die Person der die Daten zuzuordnen sind ist nicht präsent und eine Zuordnung kann nie stattfinden.
- Beschreibung des Patentes „No-Identity" Präventionskarte:
- [0017] In der 1 wird ein schematisches Flussdiagramm der „No-Identity" Präventionskarte gezeigt. 1 Position 1 des Flussdiagramms der zukünftige Nutzer bestellt das „No-Identity" Präventionskarten Paket gemäß 3: 3 Position 1 die „No-Identity" Chipkarte blank ohne Information 3 Position 2 den Fingerabdruckscanner 3 Position 3 der Kartenleser der Chipkarte 3 Position 4 die Software CD oder Memory-Stick mit Software 3 Position 5 der Heimcomputer
- [0018] Das Paket 1 Pos. 2 wird zugestellt, der Nutzer öffnet das Paket und schließt den Kartenleser 1 Position 4 oder (3 Position 3) an seinen Heimcomputer 1 Pos. 3 an. Das Internet ob WLAN oder Festverbindung muss ausgeschaltet werden. Als nächster Schritt wird die Software CD oder Memory Stick 3 Pos 4/4a in den Heimcomputer 3 Position 5 eingesteckt. Der Computer 1 Pos 3 im Flussdiagramm wird auf Neustart geschaltet und startet nun die Software 3 Pos. 4/4a im „Safemode. Damit wird sichergestellt, das weder Viren noch eine eventuelle Spionagesoftware bei der Codevergabe einen Einblick haben könnte. Die Software 3 Pos 4/4a fordert den Nutzer auf einen 17 Stellen Code in das blinkende Feld einzutragen. Dabei sollen im Laufe der Zahlenfolgen an beliebiger Stelle die Zahl mit einem Buchstaben 4 × ausgetauscht werden. Ist der Zahlencode korrekt gemäß Anleitung eingegeben wird die Eingabetaste gedrückt. Der Code wird verschlüsselt (encryptet) und auf die leere Chipkarte 3 Pos 1 über den Kartenleser 3 Pos. 3 aufgezeichnet 1 Pos. 5. Als nächste Abfolge wird der Nutzer über die Software 3 Pos 4/4a aufgefordert in das blinkende Feld einen 4 Stellen Geheimcode 1 Pos. 6 einzugeben. Danach wird die Eingabetaste gedrückt, es erfolgt die Aufforderung den Fingerabdruckscanner 3 Pos. 2 an den Heimcomputer 3 Pos. 2 anzuschließen. Als nächstes wird der Nutzer aufgefordert den rechten Zeigefinger einzuscannen. Damit wird die angelieferte blanke Chipkarte 3. Pos. 1 zur Präventionskarte 1 Pos 5 Diese Karte enthält drei Informationen:
  - 1.) einen verschlüsselten desaktivierten 17 Stellen Code (13 Zahlen 4 Buchstaben)
  - 2.) ein Aktivierungssystem das bei Eingabe von Fingerabdruck und Geheimzahl 1 Pos. 6 den verschlüsselten Code freigibt
  - 3.) ein Timer-Chip, der diesen Code nur für maximal 2 Stunden aktiv hält und nach Ablauf der Zeit den Code wiederum desaktiviert in einen verschlüsselten unbrauchbaren Zustand.
-

- [0019] Gemäß dem Flussdiagramm 1 Pos. 7 muss der eingegebene Code von der Datenbank 1 Pos. 11 genehmigt werden. Der Code wird abgeprüft auf Vollständigkeit, ob tatsächlich 13 Dezimalzahlen eingegeben wurden und 4 Buchstaben des Alphabets. Des Weiteren wird geprüft, ob der Code einigartig ist. Die Abfolge wird genau in 4 gezeigt. Der Nutzer steckt die Präventionskarte 4 Pos 1 in die vorgesehene Kartenöffnung 4 Pos. 2. der rechte Zeigefinger 1 Pos. 3 wird an den Fingerabdruckscanner 4 Pos. 4 gelegt. Danach erfolgt die Eingabe der 4 Stellen Geheimzahl in die Tastatur 4 Pos. 5. Die Karte ist aktiviert kurzfristig den Code und vergleicht den Code in der Datenbank 4 Pos. 6. Wenn der Code genehmigt ist so leuchtet die grüne Lampe 4 Pos 8 auf, ist der Code nicht korrekt oder nicht einzigartig so leuchtet die rote Lampe 4 Pos. 7 auf und die Karte 4 Pos 1 ist in diesem Fall nicht zugelassen. Bei roter Lampe 4. Pos 7 wird es notwendig sein am Heimcomputer 1. Pos 3 den Code leicht zu verändern und nochmals von der Datenbank 4 Pos. 6 bzw. (1. Pos. 11) prüfen zu lassen. Mit der nun autorisierten und desaktivierten Präventionskarte 1 Pos. 5 geht der Nutzer zu seiner diagnostischen Untersuchung. Zunächst muss die Präventionskarte aktiviert werden. Dies geschieht gemäß Flussdiagramm in 1 Pos. 8. Die Selbstaktivierung erfolgt in einem geschlossenen Computersystem des Diagnosezentrums. Hier wird sichergestellt dass auch tatsächlich der Nutzer der Besitzer der Präventionskarte ist und nur in diesem Fall ist eine Aktivierung des Codes möglich. Der Nutzer gibt seine Präventionskarte 5 Pos. 1 in den Kartenleser 5 Pos. 2 und legt seinen rechten Zeigefinger 5 Pos. 3 an den Fingerabdruckscanner 5 Pos. 4. Er gibt danach in der Tastatur 5 Pos 5 seinen 4 Stellen Geheimcode ein. Die Karte wird aktiviert. Der Code wird entschlüsselt und aktiviert über den eingebauten Timer-Chip für maximal 2 Stunden. Im Flussdiagramm 1. Pos. 9 erfolgt die medizinische Datenaufnahme im Diagnosezentrum. Während der Diagnose 6 Pos. 1 im diagnostischen Garten (in vivo, in vitro) werden an jeder Diagnosestation 1 Pos 2–12 die medizinischen Daten mit dem Code der Karte versehen. Alle medizinischen Daten die während der Diagnose 1 Pos 1 erfasst wurden werden dann in der Datenbank 6 Pos. 16 gebündelt als Paket gespeichert. Erfolgen später neue Untersuchungen oder Ergänzungen, so werden diese dem gleichen Code zugeordnet. Im Flussdiagramm werden die Daten auf der Datenbank 1 Pos. 11 abgespeichert ohne Identität nur mit dem aufgezeichneten Präventionscode 1 Pos. 10. Sowohl autorisierte Forschung 1 Pos. 19 und autorisierte medizinische Betreiber 1 Pos 17 haben Zugriff zur Datenbank, um die gebündelten medizinischen Daten auszuwerten zu analysieren oder für die Forschung zu verwenden. Die Daten können zu keinem Zeitpunkt einer Person zugeordnet werden. 6 Pos. 17 zeigt die medizinische Auswertung die Zugriff zu den Daten hat, die auf der Datenbank 6 Pos 16 gespeichert sind. Nach

ordnungsgemäßer Auswertung werden die bewerteten organisierten und ausgewerteten medizinischen Daten in einer Kartei zurück in der Datenbank 6 Pos. 16 gespeichert. Der Nutzer hat nun die Daten in seinem Durchlauf im Diagnosezentrum von einer Station zur anderen mit Hilfe seiner aktivierten Präventionskarte seine medizinischen Daten mit dem Präventionscode gekennzeichnet. Es erfolgt nun gemäß dem Flussdiagramm der Besuch des Nutzers beim vertrauten Arzt 1 Pos. 12. Erst in der Arztpraxis im Beisein des Nutzers wird es möglich sein die medizinisch ausgewerteten Daten des Nutzers auf den Bildschirm des Arztes zu holen und zwar nur während des Gespräches mit dem Arzt kann eine eindeutige Zuordnung der medizinischen Daten zum Nutzer erfolgen. 1 Pos 13 des Flussdiagramms erfolgt zunächst die Aktivierung der Präventionskarte für diesmal maximal 1 Stunde auf dem Timer-Chip. Die Karte wird über 1 Pos. 6 aktiviert. Die ausgewerteten medizinischen Daten 1 Pos. 16 von der Datenbank 1 Pos 11 fließen von der Datenbank über die aktivierte Präventionskarte 1 Pos 13 auf den Bildschirm des Arztes 1. Pos. 15. Es erfolgt danach im Flussdiagramm das Gespräch Arzt und Nutzer 1 Pos. 14. Aus diesem Gespräch ergibt sich dann ein zugeordnetes individuelles Präventionsprogramm 1. Pos. 18. Der Arztbesuch wird nun im Detail in 7 dargestellt. Über den Kartenleser 7 Pos. 1 und einen separaten Fingerabdruckscanner 7 Pos. 2 wird der Präventionskartencode für 1 Stunde über den integrierten Timer-Chip 7 Pos. 3 aktiviert. Dies ist ausreichend für ein umfangreiches Gespräch. Die gespeicherten Daten auf der Datenbank 7 Pos. 4 werden mit dem gleichen Präventionscode auf dem Bildschirm des Arztes 7 Pos. 5 angezeigt. Das Gespräch und ein Präventionsprogramm auf der Basis der medizinischen Daten kann ermittelt werden und können dem Nutzer und Arzt im persönlichen Gespräch von Nutzen sein. 8 zeigt eine typische medizinische Präventionsdatei 8 Pos. 1 Oben links 8 Pos. 2 ist der Präventionscode geschrieben. Wenn der Patient (Nutzer) anwesend ist und die Präventionskarte aktiviert 8 Pos 3 hat so erscheint die Präventionskarte als Symbol 8 Pos 3 ebenfalls im linken Feld unter dem Präventionscode 8 Pos. 2.

Claims (10)

1 Chip Karte als sicherer elektronischer Schlüssel für medizinische Daten
2 Selbstaktivierung über Geheimzahl und Fingerabdruck
3 Aktivierung zeitlich begrenzt über Timer-Chip auf Karte
4 Code Verschlüsselung bei automatischer Desaktivierung durch Timer-Chip
5 Sicherer Datenfluss durch Präventionskartenschlüssel
6 Sicherer Zugang über Chip Karte an medizinische Daten
7 Klare Zuordnung medizinischer Daten zum Karteninhaber bei eigener Präsenz nur und ausschließlich möglich
8 Methode des Aktivierungsprozesses
9 Methode der sicheren Codierung der Karte über Software im Safemode
10 Nutzung der medizinischen Daten in der Forschung ohne Daten einer

Person zuordnen zu können

Similar Documents

Publication	Publication Date	Title
Packer et al.	1959	Therapeutic abortion: A problem in law and medicine
Rose	1996	Psychiatry as a political science: advanced liberalism and the administration of risk
Mohr et al.	2008	The effect of telephone-administered psychotherapy on symptoms of depression and attrition: a meta-analysis
Lyne et al.	2000	A psychometric re-assessment of the COPE questionnaire
Grove et al.	1996	Comparative efficiency of informal (subjective, impressionistic) and formal (mechanical, algorithmic) prediction procedures: The clinical–statistical controversy.
Morrison et al.	1998	Physicians disciplined by a state medical board
Krause	1999	Reconceptualizing informed consent in an era of health care cost containment
Sugarman et al.	1998	What patients say about medical research
Gossop et al.	1999	Methadone treatment practices and outcome for opiate addicts treated in drug clinics and in general practice: results from the National Treatment Outcome Research Study.
Roberts et al.	1987	A history of the Joint Commission on Accreditation of Hospitals
Wells	1999	The design of Partners in Care: evaluating the cost-effectiveness of improving care for depression in primary care
Lewis	2006	A mad fight: Psychiatry and disability activism
Appelbaum et al.	1989	Tarasoff and the researcher: Does the duty to protect apply in the research setting?
Daniels et al.	1998	Last chance therapies and managed care pluralism, fair procedures, and legitimacy
US20110082794A1	2011-04-07	Client-centric e-health system and method with applications to long-term health and community care consumers, insurers, and regulators
Annandale et al.	1998	Accounts of disagreements with doctors

Metzner	2002	Class action litigation in correctional psychiatry
Snibbe et al.	1989	Burnout among primary care physicians and mental health professionals in a managed health care setting
DE102004051296B3	2006-05-11	Computersystem und Verfahren zur Speicherung von Daten
Pope et al.	2007	Ethical considerations for research involving prisoners
US20060229919A1	2006-10-12	Internet medical information system (IMED)
Tovino	2006	Functional neuroimaging information: A case for neuro exceptionalism
Pellegrino	1993	Societal duty and moral complicity: the physician's dilemma of divided loyalty
Polcin	2001	Drug and alcohol offenders coerced into treatment: A review of modalities and suggestions for research on social model programs
Bongar et al.	1992	Outpatient standards of care and the suicidal patient

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
DE200910050291	2009-10-15	2009-10-15	"No-Identity" Präventionskarte

Applications Claiming Priority (1)

Application	Filing date	Title
DE200910050291	2009-10-15	"No-Identity" Präventionskarte

Legal Events

Date	Code	Title	Description
2011-05-26	8122	Nonbinding interest in granting licenses declared	
2012-08-09	R119	Application deemed withdrawn, or ip right lapsed, due to non-payment of renewal fee	**Effective date**: 20120501