(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
25. Januar 2018 (25.01.2018)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2018/015409 A1

(51) Internationale Patentklassifikation:
G06F 21/32 (2013.01) *H04L 9/08* (2006.01)
G06F 21/62 (2013.01) *H04L 9/32* (2006.01)
H04L 9/00 (2006.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/068169

(22) Internationales Anmeldedatum:
18. Juli 2017 (18.07.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
00913/16 18. Juli 2016 (18.07.2016) CH

(71) Anmelder: **FUTUREITCOM GMBH** [CH/CH]; Gartenstrasse 2, 6304 Zug (CH).

(72) Erfinder: **PUTRINO, Nunzio**; Bruderholzstrasse 65, 4053 Basel (CH).

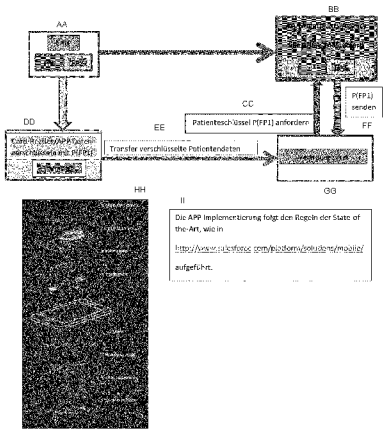
(74) Anwalt: **LEIMGRUBER, Fabian**; ThomannFischer, Elisabethenstrasse 30, 4010 Basel (CH).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

(54) **Title:** ENCRYPTION-DECRYPTION ENGINE FOR HANDLING SENSITIVE PATIENT DATA, AND CORRESPONDING METHOD

(54) **Bezeichnung:** ENCRYPTION-DECRYPTION ENGINE ZUR HANDHABUNG SENSITIVER PATIENTENDATEN UND ENTSPRECHENDES VERFAHREN



AA CHIP FP1 FP2
BB AA-Fingerprints-Agency like VISA, Mastercard
CC Request patient key P(FP1)
DD Encrypt card reader/app data with P(FP1)
Patient
EE Transfer encrypted patient data
FFSend P(FP1)
GG Fiduciary doctor
HH 8. USER EXPERIENCE
7 OFFLINE SYNCING
6. DATA LAYER
5. CONTAINER
4. SECURITY
3. BUSINESS LOGIC
2. COLLABORATION
1. BACK-END DATA
II. App implementation follows the rules of the state of the art as indicated in http://www.salesforce.com/platform/solutions/mobile/

Fig. 2

(57) **Abstract:** A biometric, fingerprint-based encryption-decryption engine for the controlled handling and secure transmission of personal, sensitive data is proposed, together with a corresponding method. A mobile communications device is used to acquire biometric data from an originator and from a confidant, in particular a set of two different fingerprints (P-FP1/P-FP2 and M-FP1/M-FP2) from each. The fingerprints (P-FP1/P-FP2) are stored in a SIM card of the mobile communications device. The first fingerprint (P-FP1/M-FP1) is assigned to authentication and the second fingerprint (P-FP2/M-FP2) is assigned to authorisation, the second fingerprint (P-FP2/M-FP2) being used to encrypt the personal, sensitive data. A learning machine of the confidant and the fingerprints are used to decrypt, mask and/or anonymise personal, sensitive data transmitted by the patient and to provide said data to third parties for the appropriate diagnosis and/or determination of medication and/or treatment.

(57) **Zusammenfassung:** Vorgeschlagen wird ein biometrischer, fingerprint-basierter Encryption-Decryption Engine zur kontrollierten Handhabung und gesicherten Übertragung personifizierter, sensibler Daten und ein entsprechendes Verfahren. Mittels eines Mobilfunkgeräts werden biometrische Daten eines Originators und eines Confidants, insbesondere jeweils ein Set von 2 unterschiedlichen Fingerabdrücken (P-FP1/P-FP2 und M-FP1/M-FP2), erfasst. Die Fingerabdrücke (P-FP1/P-FP2) werden in einer SIM-Karte des Mobilfunkgerätes abgespeichert. Der erste Fingerprint (P-FP1/M-FP1) wird der Authentisierung und der zweite Fingerprint (P-FP2/M-FP2) der Autorisierung zugeordnet wobei der zweite Fingerprint (P-FP2/M-FP2) zur Verschlüsselung der personifizierten, sensiblen Daten verwendet wird. Mittels einer Learning Machine des Confidants und mittels der Fingerprints werden vom Patienten übertragene, personifizierten, sensiblen Daten entschlüsselt, maskiert und/oder anonymisiert, und Dritten zur entsprechenden Diagnostik und/oder Festlegung der Medikamentierung bzw. Therapierung zur Verfügung gestellt.

[Fortsetzung auf der nächsten Seite]

WO 2018/015409 A1

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Encryption-Decryption Engine zur Handhabung sensitiver Patientendaten und entsprechendes Verfahren

Technisches Gebiet

Die vorliegende Anmeldung betrifft einen Encryption-Decryption Engine, insbesondere einen Fingerprint-basierten Encryption-Decryption Engine, zur Handhabung sensitiver Daten, wie dem Transfer von Patientendaten. Insbesondere betrifft sie die technische Handhabung von vertraulichen Patientendaten im Bereich der personifizierten, digitalisierten Medizin, sowie der technischen Art, ob und wie Privacy, Secrecy, maskierte Identität einer Person für die Rückverfolgbarkeit und der damit verbundenen Anonymität der persönlichen Daten, sowie Schutz vor Missbrauch der Identität einer Person im gesamten Transfer- und Lebenszyklus der Daten ermöglicht werden kann. Auf diesem Gebiet sollen derartige Verfahren oder Methoden unabhängig von Datenhintergrund oder -verwendung anwenden lassen, wenn es darum geht sensitive oder sogar hoch-sensitive Daten und/oder Informationen von einem „Provider“ oder „Producer“ an einem bestimmten „Consumer“ und/oder bestimmte „Consumer-Gruppe“ zu senden. Der umgekehrte Weg, um also von „Consumer-Gruppe“ und/oder bestimmten „Consumer“ sensitiven Daten zu einem „Provider“ oder „Producer“ zu transferieren, wird von diesen Verfahren typischerweise auch erfasst. Bei diesen Systemen dient die maskierte Identität für die Rückverfolgbarkeit eines „Producers“ und der direkten involvierten, beteiligten „Consumers“, um zusätzlich zur Privacy und Secrecy die Anonymität eines „Producers“ und/oder der direkt involvierten beteiligten „Consumers“ entlang des gesamten Lebenszyklus eines bestimmten Daten-, und Informationsflusses und Transfer in beiden Richtungen geheim zu halten. Darüber hinaus betrifft es das Gebiet der Verschlüsselung von sensitiven Daten zwischen einem Originator oder Patient und einem Confidant oder Arzt, welche die Grundsätze von Privacy, Secrecy und Anonymität der persönlichen Daten garantiert, sowie weiteren Dritten mit ausschliesslichem Zugriff auf die inhalt-bezogenen Daten und Informationen von anonymisierten und/oder mit maskierter Identität eines Originators versehene Daten, insbesondere betreffend Fälle, bei welchen der Transfer von sensitiven Daten in beiden Richtungen streng geheim zu halten ist. Die Person-bezogenen Daten sind von der Quelle eines Originators an, streng

von den inhaltbezogenen Daten und Informationen eines Originators getrennt. Die inhaltbezogenen Daten sind durch einen oder mehreren pseudo-persönlichen, zufällig generierten biometrischen Schlüssel für die Rückverfolgbarkeit und Anonymität eines Originators markiert bzw. durch die maskierte Identität gekennzeichnet und stehen stellvertretend für die personenbezogenen, d.h. personifizierte, Daten.

Stand der Technik

Schulmedizin oder andere Gebiete zur Heilung der Gesundheit stossen zurzeit an Grenzen, welche über die herkömmliche Diagnostik und Therapierung hinausgeht, was sich z.B. daran zeigt, dass zur Behandlung spezieller Krankheit Therapierungen und Medikamentierungen komplex und nach der trial-and-error Methode verschrieben werden, basierend auf der Erkenntnis bei diesen Krankheiten, dass Medikamente, welche bei Patient A Wunder wirken bei Patient B nutzlos, wenn nicht sogar fatal sein können. So werden Krankheitsbilder, wie „Orphan Disease“ meistens mit off-label-Medikamente oder chronisch kranke Patienten mit sporadischen, zusammenhanglosen Untersuchungen behandelt. Es fehlt bei diesen Arten von Krankheiten die ganzheitliche Erfassung aller diagnostisch relevanten Elemente eines Individuums seitens der Gesundheitsversorger und Leistungserbringer. Dies ist für die betroffenen Patienten, Ärzte, Krankenversicherer und im meist unvermeidlichen Streitfall (z.B. wenn es um Haftung für fälschlich angeordnete Therapien oder um Begleichung von Rechnungen geht, welche nicht in den Spezialitäten-Listen und/oder Ähnlichem aufgeführt werden, obwohl jedoch oft gerade off-label Medikamente und/oder Therapien für einen speziellen Fall wirksam sein können) einberufene Richter häufig problematisch.

Eine Möglichkeit, diese Nachteile zu umgehen und über die klassische Schulmedizin hinaus Patienten spezifisch und/oder ganzheitlich und mit der breit möglichsten Unterstützung der Spitzenforschung in direktem und/oder indirektem Zusammenwirken von betroffene(n) Patient/Patientin, behandeln zu können, bietet die sog. personalisierte Medizin, wonach Medikamente, Therapien, Behandlungen u.v.n.m. auf ein bestimmtes, personifiziertes Krankheitsbild abgestimmt werden. In der personalisierten Medizin (personalised medicine) wird jeder Patient unter weitgehender

Einbeziehung individueller Gegebenheiten, über die funktionale Krankheitsdiagnose hinaus, behandelt. Das schließt auch das fortlaufende, individualisierte Anpassen der Therapie an den Gesundungsfortschritt ein. Wichtigstes Einsatzgebiet der personalisierten Medizin ist zurzeit die massgeschneiderte Pharmakotherapie, welche zusätzlich zum speziellen Krankheitsbild die individuelle physiologische Konstitution und geschlechtsspezifische Wirkeigenschaften von Medikamenten berücksichtigt. Aber auch besonders in komplexen Therapien werden mit der personalisierten Medizin über die klassische Diagnostik und Therapierung der Schulmedizin hinausgehend ausserdem individuelle molekularbiologische Konstellationen berücksichtigt, die z.B. mit modernen Biomarkern ermittelt werden und unter denen zusätzlich zur individuellen genetischen Struktur (Genom) des Patienten auch die Ausgestaltung der Enzyme und/oder Proteine (Proteomics) und/oder Metabolomics eine gesonderte Rolle spielen. Beispielsweise können obwohl eineiige Zwillinge das gleiche Genom besitzen, aus der Sicht der Proteomics und/oder Metabolomics jedoch verschieden sein. Der Einfluss des Genoms, der Proteomics, der Metabolomics und der Biopsyen auf die Wirkung von Arzneimitteln, sowie mögliche toxikologische Auswirkungen ist Forschungsgegenstand der Pharmakogenomik als Teil der personalisierten Medizin.

Um das Ziel einer individuell abgestimmten Diagnostik, Medikamentierung und Therapierung zu erreichen, ist es unvermeidlich, persönliche Daten zu sammeln, zu untersuchen, an unterschiedliche Kompetenzzentren zu übertragen bzw. zu transferieren und unterschiedlichen Fachleute Zugriff auf die Daten zu gewähren. Zusätzlich sind auch Daten aus dem kontinuierlichen oder periodischen Monitoring, Historie, Vererbungen und Zeitreihenanalyse eines Individuums zu berücksichtigen, um für das personenbezogene Krankheitsbild Informationen und Wissen zu gewinnen. Erst dieses kollektive Zusammenwirken erlaubt eine möglichst ganzheitliche Betrachtung eines Individuums, um gestützt auf medizinische Evidenz, Wirksamkeit und Wirtschaftlichkeit die optimale Medikamentierung, Therapierung und das optimale Heilungsverfahren zu ermitteln. Aber nicht nur die Kompetenzvoraussetzungen verlangen bei der personalisierten Medizin häufig ein Einbezug mehrerer verschiedener Fachleute, sondern auch die technischen Voraussetzungen. So stellt heute noch die Analyse der gewonnenen diagnostischen Daten meist eine beachtliche Herausforderung der personalisierten Medizin dar. Z.B. fordern genetische Daten, gewonnen aus Verfahren wie dem Next-Generation Sequencing, Daten aus der Proteomics, der Toxikologie und/oder der Metabolomics, rechenaufwendige

Datenverarbeitungsschritte und sinnvolle Verknüpfungen zwischen den Daten, bevor die eigentliche Analyse der Daten erfolgen kann. Um hierbei künftig auf passende Werkzeuge zurückgreifen zu können, ist die interdisziplinäre Zusammenarbeit von Experten aus verschiedenen Gebieten erforderlich: Medizinern, klinischen Onkologen, Biologen, Softwareingenieuren, Analytiker.

Um dieser Problematik zu begegnen, gibt es verschiedene Systeme im Stand der Technik. So hat z.B. Nexus (www.nexus.ethz.ch/about.html) eine interdisziplinäre Plattform realisiert. Sie verbindet klinische Bioinformatik mit vollautomatisiertes Screening, vergleicht Resultate mit chemischen und Genom Bibliotheken. Um die Datensicherheit zu garantieren, muss jedoch Nexus nach jeder Untersuchung die untersuchten Daten löschen (siehe www.nexus.ethz.ch/collaboration/data_retention.html: "Data from approved projects will be kept on the NEXUS servers for 6 months after the date of the joint final meeting of the corresponding project. After an expiry warning to the registered project lead, the data will be removed. Given special circumstances the data lifetime cycle can be extended. Extensions will be charged according to size of the data and storage duration."

Technische Aufgabe

Es ist Aufgabe der Erfindung, eine technische Lösung bereit zu stellen, die die oben diskutierten Nachteile nicht aufweist. Die Lösung soll es dabei erlauben, die Privacy und Secrecy der Patienten durch vollkommen maskierter, rückverfolgbarer Identitätsschutz und Anonymität individuell schützen zu können. Dabei sollen es die technischen Mittel erlauben, insbesondere die gewünschten ethischen, moralischen Prinzipien und gesetzlichen Regeln zu wahren und einzuhalten. Auf der anderen Seite soll es die Erfindung ermöglichen, die persönlichen Daten einfach in den entsprechenden Forschungs-, und Entwicklungszentren zu nutzen und zu transferieren, um, aus den Krankheits-Muster personifizierte, Patient-bezogene Heilungsmöglichkeiten, Informationen und Wissen zu gewinnen. Damit soll es die Erfindung ermöglichen, schnellst möglich, mit höchstmögliche Treffsicherheit für die betroffene Person die individualisierte Therapierung und Medikamentierung zu planen und die entsprechende

weitgehende Diagnostik durch die dezentralisierte Verwendbarkeit der Daten zu ermöglichen.

Zusammenfassung der Erfindung

Gemäss der vorliegenden Erfindung werden die obgenannten Aufgaben insbesondere durch die Anspruchsmerkmale der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen können durch die abhängigen Ansprüche und die Beschreibung erhalten werden.

Gemäss der vorliegenden Erfindung werden die obgenannten Aufgaben für einen biometrischen, fingerprints-basierten Encryption-Decryption Engine zur kontrollierten Handhabung und gesicherten Übertragung personifizierter, sensibler Daten insbesondere dadurch gelöst, dass mittels eines Mobilfunkgeräts biometrische Daten eines Originators erfasst werden und in einer SIM-Karte des Mobilfunkgerätes abgespeichert werden, dass zwei unterschiedliche Fingerprints (P-FP1/P-FP2) von zwei verschiedenen Fingern des Originators mittels des Mobilfunkgeräts erfasst und in der SIM-Karte des Mobilfunkgeräts dem Originator zugeordnet abgespeichert werden, wobei der erste Fingerprint (P-FP1) der Autorisierung und der zweite Fingerprint (P-FP2) der Authentisierung zugeordnet wird, und wobei der zweite Fingerprint (P-FP2) zur Verschlüsselung der personifizierten, sensiblen Daten verwendet wird, dass die zwei Fingerprints (P-FP1/P-FP2) an einen zentralen Zugriffsserver (AAA) oder Trust Center übermittelt und dem Originators zugeordnet in einer Datenbank des Zugriffsservers abgespeichert werden, dass zwei Fingerprints (M-FP1/M-FP2) eines Confidants an den zentralen Zugriffsserver (AAA) übermittelt und dem Confidant zugeordnet in der Datenbank des Zugriffsservers abgespeichert werden, dass das Mobilfunkgeräts ein Daten-Verschlüsselungs- und -Transfermodul umfasst, wobei das Daten-Verschlüsselungs- und -Transfermodul mittels des Mobilfunkgerätes für den Originator zugreifbar ist und wobei entsprechende personifizierte, sensible Daten vom Originator mittels des Daten-Verschlüsselungs- und –Transfermodul aggregierbar und/oder validierbar und verschlüsselbar und über das Trust Center den Confidant über einen Datenübertragungskanal eines Datenübertragungsnetzwerkes transferrierbar sind, dass die transferierten Daten vom Trust Center mittels einer Learning Machine und mittels des

zweiten Fingerprints (P-FP2) des Originators entschlüsselt werden, wobei mittels der Learning Machine personenrelevante Daten der transferierten personifizierten, sensiblen Daten maskiert und/oder anonymisiert werden, und wobei mittels der Learning Machine die maskierten und/oder anonymisierten Daten mittels des Fingerprints (M-FP1) des Confidant verschlüsselt mindestens teilweise an den Confidant und/oder Netzwerk-Nodes Dritter transferiert werden, und dass die auf den Confidant oder die Netzwerk-Nodes Dritter transferierten, maskierten und/oder anonymisierten Daten durch den Confidant und/oder mittels der Netzwerk-Nodes der Dritten basierend auf dem Fingerprint (M-FP1) des Confidant entschlüsselt werden. Der Confidant, der Originator und das Trust Center bezeichnen dabei elektronische, automatisierte Vorrichtungen mit den entsprechend realisierten elektronischen Komponenten (Verschlüsselungs-/Entschlüsselungseinheit, Dateninterfaces, Speicher etc.) Insbesondere beim Originator ein Mobilfunkgerät oder einen mobilen Netzwerknode und beim Confidant einen Netzwerknode als solchen. Als Variante können mittels eines Mobilfunkgeräts biometrische Daten eines Originators erfasst werden und in einer SIM-Karte und/oder innerhalb eines gesicherten Ordners im Filesystems des Mobilfunkgerätes und/oder End-Nutzer-Gerätes abgespeichert werden, dass zwei unterschiedliche Fingerprints (P-FP1/P-FP2) und/oder biometrische Messungen (B-MM1 /B-MM2) von zwei verschiedenen Fingern und/oder Körperteilen des Originators mittels des Mobilfunkgeräts und/oder Erfassungsgeräts für biometrische Messungen erfasst und in der SIM-Karte und/oder innerhalb eines gesicherten Ordners im Filesystems des Mobilfunkgeräts und/oder End-Nutzer-Gerätes dem Originator zugeordnet und abgespeichert werden, wobei der erste Fingerprint (P-FP1) oder die erste biometrische Messung (B-MM1) der Autorisierung und der zweite Fingerprint (P-FP2) und/oder die zweite von der ersten unabhängige, biometrische Messung B-MM2 der Authentisierung zugeordnet wird, und wobei der zweiten Fingerprint (P-FP2) zur Verschlüsselung der personifizierter, sensibler Daten verwendet wird, dass die zwei Fingerprints (P-FP1/P-FP2 bzw. B-MM1 /B-MM2) an einen zentralen Zugriffsserver (Authentication, Autorisation, Accounting (AAA)) übermittelt und dem Originators zugeordnet in einer Datenbank des Zugriffsservers abgespeichert werden, dass zwei Fingerprints (M-FP1/M-FP2) eines Confidants an den zentralen Zugriffsserver (AAA) übermittelt und dem Confidant zugeordnet in der Datenbank des Zugriffsservers (mittels des im Folgenden beschriebenem Regelwerkes) abgespeichert werden, dass das Mobilfunkgeräts ein Daten-Verschlüsselungs- und -Transfermodul umfasst, wobei das Verschlüsselungs- und -Transfermodul mittels des Mobilfunkgerätes für den Originator zugreifbar ist und wobei entsprechende personifizierte, sensible

Daten vom Originator mittels des Verschlüsselungs- und –Transfermodul aggregierbar und/oder validierbar, verifizierbar und verschlüsselbar und an den Confidant über einen sicheren, verschlüsselten Datenübertragungskanal eines Datenübertragungsnetzwerkes (wie z.B. einem Virtual Private Network (VPN)) transferrierbar sind, dass die transferierten Daten vom Confidant mittels einer Learning Machine und mittels des zweiten Fingerprints (P-FP2) des Originators entschlüsselt werden, wobei mittels der Learning Machine und/oder Deep Learning Machine und/oder künstlichen Intelligenzmodule personenrelevanten Daten der dazugehörigen, eineindeutigen, inhalt-bezogenen, transferierten, personifizierten, sensiblen Daten (nach Verifizierung und Validierung der sowohl in den Person-bezogenen als auch in den eineindeutigen, zugehörigen Inhalt-bezogenen Daten vorhandenen und mittels der identischen in beiden Datenarten eingebetteten Autorisierungsschlüssel übereinstimmend zusammenfügten Daten) maskiert und/oder anonymisiert werden, und wobei mittels der Learning Machine und/oder Deep Learning Machine und/oder künstlichen Intelligenzmodule die maskierten und/oder anonymisierten Daten mittels des Fingerprints (M-FP1) des Confidants (der Confidant bildet für das darauffolgende Transfer der sensiblen Daten auch Originator) verschlüsselt mindestens teilweise an Netzwerk-Nodes Dritter transferiert werden, und dass die auf die Netzwerk-Nodes Dritter transferierten, maskierten und/oder anonymisierten Daten mittels der Netzwerk-Nodes basierend auf dem Fingerprints (-M|CFP2) des Originator (M)/(C) entschlüsselt werden. Der erfindungsgemässe biometrischen Encryption-Decryption Engine hat u.a. die Vorteile, dass einerseits die Privacy, Secrecy und maskierte Identität und Anonymity der Patienten nach ethischen, moralischen Prinzipien und gesetzlichen Regeln einfach gewahrt werden können. Anderseits, können die Daten mit maskierter Identität oder die anonymen, verschlüsselten Daten, von den Quellen zu den Forschungs-, und Entwicklungszentren problemlos genutzt werden (entweder mit der maskierten Identität für die Rückverfolgbarkeit oder absolut anonym, mit Verlust der Rückverfolgbarkeit), wobei insbesondere aus den Krankheits-Muster patienten-bezogene Heilungsmöglichkeiten, Informationen und Wissen gewonnen werden kann. Die mit dem biometrischen Marker eines Originators als auch des zugehörigen Confidants maskierten Identitäten und verschlüsselten Daten sind für ein spezielles Individuum somit rückverfolgbar. Damit ist es möglich schnellstens, mit höchstmöglicher Treffsicherheit für die betroffene Person die entsprechende personifizierte Medikamentierung und Therapierung zu planen, wobei sich diese aufgrund eines kontinuierlichen Monitorings einer betroffenen Person insbesondere dynamisch und zeitabhängig ändern und/oder

anpassen lassen, wenn die entsprechenden, individuell eingestellten Parameter technisch mittels Learning Machine getriggerte oder anderweitig überwachte Schwellwerte erreichen. Damit lassen sich auch Konstellationen automatisiert abfangen, die für Patienten toxikologische oder die Fortsetzung der Medikamentierung und/oder Therapierung für die betroffene Person fatale Folgen haben können.

Die Erfindung erlaubt z.B. heutige mobile Geräte für diese Zwecke sinnvoll zu nutzen, meist ohne weitere Modifikation. In Fig. 1 wird am konkreten Beispiel mit FPC-Sensoren https://www.fingerprints.com/technology/hardware/fpc1020/ und in Fig.2 mit einem konkreten Fall gezeigt wie ein mobiles Gerät für das Vorhaben sinnvoll Modifiziert werden kann, dies gilt ebenso für hochwertige Sensoren, wie für Gesichtserkennung, z. B. http://eu.mouser.com/new/Omron-Electronics/omron-b5t-hvc-sensor/ oder Iris, Retina-Scanning, Spracherkennung, Erkennung der Handfläche-Geometrie, usw. Nachfolgend wird gezeigt wie mit wenigem Aufwand Erfassungsgeräte für biometrischen Messungen modifiziert und/oder erweitert werden können, um diese Systeme und Verfahren einzubetten. Der Confidant, insbesondere als Vertrauensarzt, kann mittels der Erfindung einerseits ad hoc und/oder on demand, orts-und zeitunabhänig alle oder spezifische Teile der persönlichen Daten und/oder die elektronischen, dezentralisierten Patientendossiers sicher, schnell und zuverlässig zusammenfügen, um ein ganzheitliches Bild der behandelten Person zu haben. Anderseits kann der Confidant zusammen mit anderen von der behandelten Person zuvor zugestimmten Confidants ad hoc und/oder on demand, orts-und zeitunabhänig alle oder spezifische Teile der persönlichen Daten und/oder die elektronischen, dezentralisierten Patientendossiers sicher, schnell und zuverlässig zusammenfügen, um ein ganzheitliches Bild der behandelten Person zu haben, um selber die Inhalt-spezifischen Daten der behandelten Person an weitere Spezialisten/Confidant(s) übermitteln und/oder die vielfältigen, dezentralisierten Patientendossiers zu einem einzigen anonymisierten und/oder verschlüsselten Patientendossier erfassen. Die Erfindung ist nicht beschränkt auf Fingerprints als biometrische Kenndaten. Für die Autorisierung der Person-bezogenen Daten und für die Authentisierung für die Verschlüsselung der Inhaltbezogenen Daten eines bestimmten Patienten bieten allgemein biometrische Erkennungen, wie Fingerprint, Gesichtserkennung oder Ausmessen/Erfassen der Iris usw. eine grosse Vielfalt an Möglichkeiten, welche in Zusammenhang mit dem erfindungsgemässen Engine anwendbar sind. Allerdings ist aus diesen Möglichkeiten die Fingerprint-Erkennung, diejenige, welche sich im Markt am

deutlichsten durchgesetzt hat und z.B. in den moderneren Smartphones bereits integriert ist. Ein Vorteil der Erfindung liegt deshalb auch darin, etablierte, technische, mehrfach erprobte, standardisierte Lösungen zu integrieren zu können, um mit geringem Aufwand eine End-to-End verlässliche, sichere Lösung vorzuschlagen, die den Anforderungen an Datensicherheit und der Ethikkommission genügt. Die Gewähr der Privacy, Secrecy und Anonymity der persönlichen Daten beginnt deshalb schon beim Originator und/oder dem Patienten.

Insbesondere kann das erfindungsgemässe System und Verfahren basierend auf allen Arten von persönlichen, biometrisch gewonnenen Messungen realisiert sein, denn es ist Kern der Erfindung, zwei unabhängige zufällig generierten, pseudo-persönlichen Schlüssel zu bestimmen, womit alle Arten von Daten, wie z.B. Video, Sprachaufzeichnungen, Bilder, Texte u.v.n.m. mit (a) einem persönlichen, biometrischen Schlüssel zu verschlüsseln und (b)die Daten mit dem zweiten, unabhängig vom ersten Schlüssel, generierten, persönlichen Schlüssel zu markieren ohne die wahren biometrischen Schlüssel je im Umlauf zu bringen und/oder die Identität eines Individuums direkt oder indirekt zu gefährden. Somit lassen sich die erfindungsgemässen Systeme und Verfahren auch länderspezifisch, oder weltweit eins-zu-eins einsetzen, in dem in einer entsprechenden Applikation, kurz APP, das System oder Verfahren die jeweiligen landesspezifischen Anpassungen, wie Sprache, Zeitzone, landesspezifische Kenn-IDs, usw. vornimmt. Erfindungsgemäss lässt sich z.B. auch ein End-Nutzer-Gerät, welches die persönlichen, biometrischen Messungen erfasst, zusätzlich als „Dolmetscher" verwenden, in welchem bei der Kommunikation die gängigen, gewünschten Welt-Sprachen Übersetzer ausgewählt und eingebunden werden. So ist es z.B. möglich jemanden um Hilfe oder in einer Notsituation dem helfenden Arzt die eigenen Patienteninformationen aus dem Ursprungsland anzuzeigen, die entsprechende, fachspezifische, automatische Übersetzung des jeweiligen Gastlandes auszuwählen und/oder mit dem Hausarzt, Spezialist oder spezialisierten Spital im Ursprungsland zu verbinden, um auch an entfernten Weltteile mittels Telemedizin von lokalen Gesundheitsfachpersonen die optimale, medizinische Versorgung zu erhalten. Diese können dann eventuelle, weitere Schritte einleiten, z.B. für die Repatriierung in das Ursprungsland.

Sämtliche Aufzeichnungen, wie Sprache (insb. Originalsprache), Video, Texte, Bilder, usw. können mittels des erfindungsgemässen Systems vom End-Nutzer-

Gerät ad hoc erfasst und z.B. verschlüsselt in das persönliche, elektronische Patientendossier im Ursprungsland gespeichert werden. End-Nutzer sind mit diesem System und Verfahren vor Missbrauch der persönlichen, biometrischen Messungen geschützt, was zum Beispiel insbesondere in autoritäre Staaten, illegale Polizeikorps, Diktatoren etc. wichtig sein kann, welche mit illegalen Mittel sich der AA-Agencies oder des End-Nutzer-Gerätes bemächtigen, und so für illegale Zwecke missbrauchen können, aber auch in Bezug auf Hacker-Gemeinden, welche z.B. Lösegelder erpressen. Der Identitätsschutz eines End-Nutzers, der wie erwähnt ein zentrales Element der Erfindung darstellt, ist gewährleistet, weil nur geheime, zufällig generierte, pseudo-biometrische, persönliche Messungen aus den echten, persönlichen, biometrischen Messungen generiert und verwendet werden, und somit an AA-Agenturen transferiert und in AA-Agenturen gespeichert werden. Der Autorisierungsschlüssel, welcher persönliche, biometrische Messungen enthält, wird erfindungsgemäss geheim generiert, und wird in die personifizierten Daten bzw. elektronischen Akten (Patienten-, Buchhaltung-, Ledger-, ...) automatisch vom System und Verfahren eingebettet. Der Autorisierungsschlüssel repräsentiert und bildet dabei geheimer Platzhalter innerhalb aller inhaltsbezogenen Daten, welche einen echten Sachverhalt beschreiben, wie z.B. klinische Patientendaten, Finanz-, oder Versicherungs-, oder Forschungs-, oder Intelligence-Daten u.v.n.m., für die personenbezogenen Daten. Die persönlichen, biometrischen Messungen des Authentifizierungsschlüssels betreffen Körperteile, welche verschieden sind von anderen biometrischen Messungen, wobei der Authentifizierungsschlüssel, wie erwähnt, geheim und/oder geschützt generiert wird, welcher für die Verschlüsselung der Daten verwendet. Die beiden verschiedenen, echten, persönlichen, biometrischen Messungen, z.B. aus zwei verschiedenen Fingerprints, bleiben immer und ausnahmslos im Device/Gerät eines End-Nutzers erhalten und geschützt gegen Eindringlinge oder Dritte aufbewahrt, indem jedweder externe Zugriff verhindert wird. Die echten, persönlichen, biometrischen Messungen (Finger, Gesicht, Iris, ...) werden dabei vom erfindungsgemässen System nie über das Netz gesendet und schon gar nicht irgendwo, ausser im eigenen End-Nutzer-Gerät, wie bereits beschrieben, gespeichert. Wichtig zu bemerken ist, dass das erfindungsgemässe System und Verfahren im Umgang mit sensitiven oder hoch-sensitiven Daten nur beispielshaft am konkreten Beispiel von Patientendaten aufgezeichnet ist. Das erfindungsgemässe System und Verfahren lässt sich auch ohne tiefgreifende Anpassungen direkt auf Datentransfer und –Schutz in der Finanz-, Versicherungs-, Intelligence- und Forschungstechnologie übertragen. Weiter ist anzumerken, dass

erfindungsgemäss die AA-Agenturen als Master-Master-hochverfügbare-Replikationsserver und nach den strengen Kriterien eines Kredit-Karten-Zentrums aufgebaut, gesichert, zertifiziert und betrieben sind.

Die vorliegende Erfindung erlaubt eine einfache Erweiterung der Algorithmen und der Fingerprint-Recognition-Technologie des Standes der Technik. Anderseits können gleichzeitig Plattformdienste und –Technologien, wie oben am Beispiel von Nexus beschrieben, integriert und realisiert werden.

Die Erfindung erlaubt persönliche Patientendaten vom Patienten verschlüsselt zu Vertrauensärzte (oder anderen Confidants) zu übermitteln und weiter mittels rückverfolgbar, maskierte Identität zu dritten Forschern oder Personen zu übermitteln. Aufgrund der maskierten Identität können in der Folge die Daten an Dritte (z.B. Forschung-, und Entwicklungseinheiten) verschlüsselt und zu einem bestimmten Krankheitsbild eines bestimmten Patienten als passenden Antworten zurück an die jeweiligen Vertrauensärzte/Confidant und von diesen an Patient/Originator, transferiert werden. Dennoch können die korrelierenden Krankheitsbilder zu den Behandlungen in einer sicheren, relationalen, schnellen Datenbank und/oder NoSQL-Datenbank und/oder Graphendatenbank aufbewahrt werden. Learning Machines oder Deep Learning Machines oder artificial-intelligence-basierte Module und/oder business-intelligence-basierte Module verarbeiten die anonymisierten und/oder die mit maskierter Identität versehenen, persönlichen Daten zu Informationen und Wissen, bewerten mit hoher Treffsicherheit individuelle Krankheits-Muster mit Medikamente, Heilungs-Verfahren und Therapien und untersuchen die möglichen toxischen Nebenwirkungen für einen speziellen Patienten. Die vorbereiteten Informationen ermöglichen, dass bei neuen Anfragen die Antworten treffsicherer und schneller gegeben werden können. Mittels Vergleich aus anderen ähnlichen Fällen können insbesondere individuelle Medikamente, Heilungs-Verfahren und Therapien an Confidant(s) treffsicher empfohlen werden.

In einer Ausführungsvariante ist der Originator ein medizinischer Patient, wobei die sensiblen, personifizierten Daten automatisiert von einer Learning Machine oder Deep Learning Machine oder Artificial Intelligence-basiertes Modul als Confidant und/oder Vertrauensarzt mittels einer Learning Machine Dritten zur weiteren Diagnostik und/oder Therapierung zur Verfügung gestellt werden. Das Mobilfunkgerät des

Originators kann z.B. mindestens einen Sensor zum Erfassen von biometrische Daten umfassen. Das Mobilfunkgerät des Originators kann durch weitere Applikationen/Programme ad hoc auch als „Dolmetscher“ und „Aufzeichnungsgerät“ verwendet, erweitert werden, und die so generierten neuen Daten verschlüsselt im elektronischen Patientendossier integrieren oder anreichern oder sogar ein neues elektronisches Patientendossier anlegen. Mittels des mindestens eines Sensors zum Erfassen von biometrische Daten können z.B. Finger-Prints als biometrische Schlüssel erfasst werden. Der zentrale Zugriffsserver (AAA) kann z.B. einer Authentisierungs- und Autorisierungs-(AA)-Agency zugeordnet sein. Der Confidant kann z.B. zur Entschlüsselung der personifizierten, sensiblen Daten mittels der Learning Machine auf die entsprechenden Fingerprints (P-FP1/P-FP2) des Originators auf dem zentralen Zugriffsserver (AAA) zugreifen und auf die Learning Machine übertragen. Die Netzwerk-Nodes Dritter können z.B. zur Entschlüsselung der maskierten und/oder anonymisierten Daten auf die entsprechenden Fingerprints (M-FP1/M-FP2) des Confidant auf den zentralen Zugriffsserver (AAA) zugreifen und auf sich übertragen.

Mittels der Learning-Machine oder Deep Learning Machine oder Artificial Intelligence-basiertes Modul können z.B. die entschlüsselten sensiblen, personifizierten, inhaltlichen Daten auf Daten-Konsistenz und Daten-Qualität überprüfbar werden. Mittels der Learning-Machine oder Deep Learning Machine oder Artificial Intelligence-basiertes Modul kann z.B. automatisiert oder durch den Confidant feingranulare Aktivierungsstufen detektiert und dem Originator zugeordnet werden, wobei basierend auf den Aktivierungsstufen die Daten den Netzwerk-Nodes Dritter zugänglich gemacht werden. Die Aktivierungsstufen kann z.B. mindestens die Triggerelemente "kein Handlungsbedarf" und/oder "Warnung" und/oder "Alarmzustand" umfassen. Es steht allerdings nichts im Weg mittels feingranularer Triggerelemente und/oder feingranularer Steuerung für die Verabreichung von Medikamente oder Erinnerungsfunktionen an Originator eine bestimmte Therapie durchzuführen und/oder ein bestimmtes Medikament einzunehmen usw. im Gegenzug Messwerte und/oder Parameter von Organen, Körperflüssigkeiten und/oder aus Scanning von Körperteilen, wie Haut, direkt von den Messgeräten mittels des eingebetteten Systems und Verfahrens, die in dieser Lösung beschrieben sind, an Confidant(s) zu senden.

Wichtig ist, dass die erwähnten Netzwerk-Nodes Dritter, insbesondere entsprechende Forschung- und Entwicklungsinstitute (F&E), einem genau bestimmten

Confidant / Vertrauensarzt Pharmako-relevante Medikamente, Therapien u.v.n.m, für ein spezielles Patienten-bezogenen Krankheitsbild übermitteln. Der Confidant oder die Learning Machine beim Confidant/Vertrauensarzt alleine ist in der Lage die mit maskierten Identität markierten, anonymisierten und encrypted Daten genau einem bestimmten Patienten zu zuweisen. Typischerweise ist es ausschliesslich der Vertrauensarzt- und nicht die Learning-Machine oder Deep Learning Machine oder Artificial Intelligence-basiertes Modul, die nach Überprüfung der vorgeschlagenen pharmako-relevante Medikamente, Therapien aufgrund des Autorisierungs-Schlüssels P(FP1) gekoppelt an den Authentifizierungs-Schlüssel P(FP2) auf den echten Patienten schliessen kann und diesen in der Folge fachgerecht benachrichtigen kann. Andere Ausführungsvarianten sind aber ebenfalls vorstellbar.

Zusammenfassend lassen sich folgende Elemente und Schritte als Kern der Erfindung festhalten:

(1) Die Grundstruktur für die mit individualisierten, biometrischen Schlüssel verschlüsselte Kommunikation von Informationen und/oder Daten und/oder Dokumente besteht aus Producer-Einheit, Trusted-Einheit oder Trusted Center und Consumer-Einheit. Die Kommunikation ist bidirektional und immer mit dem Schlüssel des/der empfangenden Consumer verschlüsselt. Jede Consumer-Einheit kann seinerseits selber Producer von einem weiteren Consumer oder von weiteren Consumers sein.

(2) Mit einem Endnutzer-Gerät erzeugen unabhängig voneinander Producers und Consumers je zwei unabhängige, individualisierte, biometrische Messungen von beliebigen Körperteilen, z. B. zwei verschiedene Fingerprints, Gesichtserkennung, Iris, usw. Die zwei unabhängigen biometrischen Messungen werden je in einen entsprechenden biometrischen Schlüssel transformiert, wobei die biometrischen Schlüssel mindestens teilweise basierend auf den biometrischen Messungen transformiert werden, z.B. mittels eines entsprechenden Transformations-Moduls oder Kryptosystems. Mindestens teilweise kann die Transformation jedoch auch auf zusätzlichen Transformations-Verknüpfungen basieren, z.B. zufälliger Permutationsalgorithmen oder symmetrischer oder asymmetrischer Verschlüsselungsalgorithmen, wie z.B. dem Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Public-Key-

Verschlüsselungsverfahren, Public-Key-Authentifizierung und/oder digitale Signaturen. Die erfindungsgemässe Transformation erlaubt eine einzigartige Zuordnung von biometrischer Messung in einen digitalen biometrischen Schlüssel, z.B. einen 256-bit oder 512-bit Schlüssel. Der erste biometrische Schlüssel dient der eineindeutigen Identifikation eines Producers. Der zweite, unabhängiger, biometrische Schlüssel dient der Verschlüsselung von Daten-Content, i.e. Informationen und/oder Daten und/oder Dokumente, die dem Producer bzw. der Producer-Einheit zugeordnet sind.

(3) Producers und Consumers senden unabhängig voneinander dem Trust-Center die individualisierten, geheimen, biometrischen Schlüssel. Ein Schlüssel für die eindeutige Zuordnung der Identität eines Producers und der zweite Schlüssel für die eindeutige Verschlüsselung eines Daten-Contents, wie Informationen, Daten, Dokumente des urhebenden Producer.

(4) Die Zuordnung bzw. Freigabe von Content-Daten an einen oder mehrere Consumer kann nur über die Producer-Einheit bzw. den Producer erfolgen, ohne dass die bidirektionale, verschlüsselte Kommunikation zwischen Producer-Consumer oder Producer-Consumers aufgegeben wird. Insbesondere kann die Freigabe über das Trusted Center erfolgen. Über das Trusted Center oder über die Producer-Einheit werden die Content-Daten wie Informationen, Daten oder Dokumente eines Producers mit einem Schlüssel des freigegebenen Consumer verschlüsselt.

(5) Eine der beiden biometrischen Schlüssel dient ausschliesslich für die Verschlüsselung der Informationen und/oder Daten und/oder Dokument. Dieser biometrische Schlüssel bleibt immer im Trusted Zentrum gespeichert und wird nie (abgesehen vom ersten Mal zwischen Producer und Trusted Center) über das Netz gesendet.

(6) Im erfindungsgemässen Datentransferverfahren ermöglichen die Contentdaten nie einen eindeutigen Rückschluss über den urhebenden Producer, i.e. dessen Identität, und/oder Consumer, der seinerseits selber gegenüber einem weiteren Consumer als urhebenden Producer wirkt, Informationen und/oder Daten, welche Rückschlüsse auf die Identität eines Producer ermöglichen. Das Trusted Zentrum wirkt als Drehscheibe, mit den Aufgaben Producer mit bestimmten vom Producer beglaubigten

Consumer oder Consumers zu zuordnen, die Content-Daten mit dem zweiten Schlüssel des urhebenenden Producers zu entschlüsseln, um sofort nachfolgend mit einem Schlüssel eines zugeordneten, und vom Producer freigegebenen Consumers zu verschlüsseln und entweder die verschlüsselten Content-Daten an den entsprechenden Consumer zu transferieren, oder den genauen Speicherort der Content-Daten und nach Bedarf des urhebenden Producers die Verwendung bzw. den Access zu ermöglichen.

(7) Content-Daten, i.e. Informationen, Dokumente und/oder Daten, eines urhebenden Producers enthalten nie Informationen, mittels welchen der Producer identifiziert werden könnte. Falls ein Dokument Identifikations-Daten und/oder Informationen enthält, dann werden diese Informationen und/oder Daten vollständig mit dem zweiten, individualisierten, biometrischen Schlüssel ersetzt. Der zweite individualisierte, biometrische Schlüssel eines urhebenden Producers dient als eindeutiger Marker eines Producers von Content-Daten.

(8) Der Ausschluss von persönlichen Identifikations-Daten eines urhebenden Producers erfolgt entweder beim End-Gerät des Producer und/oder beim Consumer, wenn dieser gegenüber weiteren Consumers die Rolle eines Producers annimmt oder im zentralen, voll-automatisierten Trusted Center. Der individualisierte, biometrische Marker dient insbesondere zur eineindeutigen Zuordnung zwischen Producer-Consumer. Damit ist die Identität eines Producers oder Identitäten von mehreren Producern (wenn Consumer zu Producern mutieren) vollkommen maskiert, wobei die korrekte beglaubigte Zuordnung von Producer und Consumer allein dem Trusted Center bekannt ist.

(9) Im erfindungsgemässen System und Verfahren können Producer mit einem Endnutzer-Gerät auf alle eigene, urheberrechtliche Content-Daten (Dokumente, Informationen, Daten) jederzeit und ortsunabhängig zugreifen. Producers verwalten vollkommen unabhängig die Granularität, d.h. die Hierarchien, der Zugriffsrechte für jeden einzelnen beglaubigten und vom Producer zugeordneten Consumer sowohl auf ein gesamtes Dokument und/oder Informationen und/oder Daten oder Teile davon.

(10) Ein Producer kann erfindungsgemäss zu eigenen Content-Daten (Dokumente, Informationen und/oder Daten) einem oder mehreren Consumer ganz

oder teilweise Zugriffe und Rechte, wie schreiben, lesen, abfragen, gleichzeitig oder einzeln gewähren. Content-Daten eines Producers können somit einen und/oder sogar mehrere individualisierte, biometrische Schlüssel von Consumer umfassen enthalten, welche nur dem Trusted Zentrum bekannt sind und im Trusted Zentrum verwaltet werden. Nur Producer und/oder solche Consumer, welche zu Producer mutieren, dürfen die Identität eines Producers mit dem zweiten Individualisten biometrischen Schlüssel ersetzen und im die Content-Daten einbetten.

(11) Ein Producer kann die Hierarchie bzw. Granularität der Zugriffe auf ein Dokument oder Teile davon jederzeit ändern ohne die beteiligten Consumer zu benachrichtigen. Umgekehrt, falls ein beglaubigter, zugeordneter Consumer eines Dokumentes, d.h. von Content-Daten, eines urhebenden Producers diese in irgendeiner Weise ändert, abfragt, liest, öffnet oder wie auch immer manipuliert kann der entsprechende Producer als Erfindungsvariante sofort benachrichtigt werden. Einträge in Dokumente und/oder Informationen und/oder Daten dürfen nur die Urheber eines Dokumentes und/oder Informationen und/oder Daten logisch löschen. Für Consumer mit den expliziten Rechte ein Dokument zu ändern, einzufügen oder zu schreiben, werden sämtliche Änderungen stets markiert und vom System getraced. Als Variante, kann eine besondere SOS- und/oder Alarm-Funktion Dritten erlauben, Dokumente bzw. Content-Daten für den Producer zu erstellen.

Kurze Beschreibung der Zeichnungen

Die vorliegende Erfindung wird detaillierter erklärt durch die folgenden Beispiele mit Referenzierung zu den Zeichnungen, wobei:

Fig. 1 zeigt schematisch den Prozessschritt 1 an einem moderneren iPhone als Mobilfunkgerät. Das kommerzielle iPhone lässt sich z.B. mittels einer Karte FPC1268 (Fingerprint-Card 1268), welche unabhängig von der Plattform unter dem Deckglas eines Smartphones montiert werden kann, für die Erfindung einrichten. Dazu können zwei Sensoren (www.fingerprints.com/products/fpc1080a-swipe/; www.fingerprints.com/products/productsarea-sensor/) im mobilen Endgeräte eingebaut werden.

Fig. 2 zeigt schematisch den Prozessschritt 3. Falls die Infrastruktur des Vertrauensarztes die Sicherheitskriterien erfüllt, können die P(FP1) und P(FP2) sicher in der IT-Umgebung gespeichert werden. Ansonsten, können die P(FP1) und P(FP2) bei einer AA-Agency gespeichert werden. Der Vertrauensarzt muss danach bei einer vertrauenswürdigen AA-Agency (Autorisierung-, Authentisierungs-Agentur) den Schlüssel P(FP2) anfordern, um die Patientendaten zu entschlüsseln. Ein Algorithmus sorgt dafür, dass beim Schliessen des elektronischen Patientendossiers (i) automatisch die Patientendaten mit dem Schlüssel des Patienten P(FP2) verschlüsselt abgelegt werden und (ii) der vom Vertrauensarzt von der AA-Agency angeforderte Schlüssel P(FP2) (Patientenschlüssel) vom lokalen IT-System des Vertrauensarztes gelöscht wird.

Fig. 3 zeigt schematisch den Prozessschritt 4. Prozessschritt 4 umfasst (i) Learning Machine maskiert alle Patient relevanten Daten (Namen, Vornamen, Geburtsdatum, Geschlecht, ...); Daten nur mit P(FP1), Autorisierungsschlüssel versehen; (ii) Anonymisierte Patientendaten mit Schlüssel des Vertrauensarztes M(FP2) verschlüsseln E(Pat-Daten; M(FP2)); (iii) Senden der verschlüsselten Daten E(Pat-Daten; M(FP2)) an ein Forschungs-, Entwicklungszentrum, z.B. Nexus.

Fig. 4 zeigt schematisch den Prozessschritt 6. Prozessschritt 6 umfasst (i) Forschungs-, und Entwicklungszentrum (F&E) fordert von der AA-Agency Schlüssel M(FP1), d.h. Medical Fingerprint für Authentifizierung, an. Die Autorisierung erfolgt mit dem Schlüssel M(FP2), d.h. Autorisierung mittels Medical Fingerprint; (ii) AA-Agency übermittelt an (F&E) den Schlüssel M(FP1). In F&E werden die verschlüsselten Patienten-Daten E(Pat-Daten; M(FP2)) mit dem M(FP2) entschlüsselt

D(E(Pat-Daten; M(FP2)) = (Pat-Daten; M(FP2))

In den Patienten-Daten ist auch den P(FP1), Autorisierungsschlüssel des Patienten enthalten. Die Learning-Machine kann dabei einen Beitrag leisten, um den Match „Krankheits-Muster" eines Patienten mit möglichen Medikamente, Therapien zu finden.

Fig. 5 zeigt schematisch die erfindungsgemässe Relation zwischen Vertrauensarzt / Patienten

Fig. 6 zeigt ein Flussdiagramm für Benachrichtigung vom F&E zum Patient.

Fig. 7-21 zeigen eine Erweiterung und Verbesserung des erfindungsgemässen Systems nach Fig. 1-6 für jede Art von individuellen, biometrisch gewonnene Messungen, anwendbar auf sensitiven oder hoch-sensitiven Datentransfer jeglicher Art und Weise, wobei unter Daten Video, Sprachaufzeichnungen, Bilder, Texte u.v.n.m., zu verstehen sind.

Fig. 7 illustriert ein Protokoll-Aufbau der gesendeten hoch-sensitiven Daten.

Fig. 8 a/b illustrieren, wie eine Applikation oder APP verschiedene Funktionalitäten enthalten kann, personenbezogene Daten nach Sensitivität trennen kann, Liste von Referenzen, Prozesse, Informationsfluss und Administration der Zugriffsrechte für die referenzierten Verbraucher. Die App kann z.B. skalierbar für End-Nutzer-spezifische Erweiterungen ausgebildet sein.

Fig. 9 zeigt ein Beispiel für CRUD Zugriff angewendet auf die Content-Daten Dokument 1 und 2. MED 1 kann z.B. leserecht (R) für Dokument 1 und nachführrecht (U= update) auf Dokument 2 erhalten. MED 2 kann z.B. Erstellrecht (C=create) für Dokument 2 erhalten, d.h. kein Zugriffsrecht für Dokument 1 usw.

Fig. 10 zeigt ein Beispiel für zwei verschiedene Fingerprints, welche verschieden Lang sein können als Repräsentant für zwei unabhängige, beliebige, zufällig generierte biometrische Schlüssel.

Fig. 11 illustriert ein Verfahren zur Erzeugung des pseudo-persönlichen-Codes.

Fig. 12 zeigt Feldnamen und minimale Anzahl der Felder für Personenbezogene Informationen.

Fig. 13 zeigt den Binary Code für jeden Text-Code aus Fig. 4.

Fig. 14 zeigt, wie ein End-Nutzer je eine zufällige Folge gibt, z.B. [4,9,0,7,6,5,2,1,8,3], ein, für jede unabhängig abgegriffene, biometrische Messung.

Fig. 15 zeigt ein Algorithmus für das Erstellen von zwei unabhängigen, Random-generierten, pseudo-persönlichen biometrischen Schlüssel.

Fig. 16 zeigt am Beispiel eine Abbildung zwischen Patienten, zugeordneter Arzt oder Ärzte und Dokumente in der AA-Agentur. Die MED_ID verbindet Patient-Arzt.

Fig. 17 zeigt beispielhaft drei Schritte, um bestehende elektronische Patientendaten mit FEDE zu betreiben.

Fig. 18 zeigt die Registrierung der MED_ID beim erstmaligen Arztbesuch.

Fig. 19 illustriert den Prozess beim Arzt/Spital/Klinik, um Fragen an R&Ds zu stellen unter Wahrung von Privacy, Secrecy und Anonymity.

Fig. 20 illustriert die Metadaten zu den Dokumenten PD_[1..m], die in Form von URL oder URI[1..q] in der AA-Agentur gespeichert sind, genau mit Patienten-Autorisationsschlüssel P[1..r](FP1) markiert und P[1..r](FP2) verschlüsselt und genau einem Leistungserbringer MED_ID[1..t] zugewiesen. Die Dokumente können in eine Cloud, bevorzugt in eine private Cloud gespeichert werden. Die URI eines Dokumentes ist dabei eineindeutig.

Fig. 21 zeigt den Zusammenhang und Abbildung zwischen MED_ID, Fragen von Ärzte an R&Ds und die Einbettung der Autorisation-Schlüssel von Patienten und Ärzte in die Fragen an R&Ds

Fig. 22 zeigt einen Decryption-Encryption-Decryption Mechanismen zur Wahrung von Privacy, Secrecy, Anonymity, um Fragen von Ärzten über bestimmte Patienten rückverfolgbar, jedoch mit maskieren Identitäten sowohl von Patienten als auch von Ärzten an bei der AA-Agency akkredierte Research und Development Laboratories zu senden.

Fig. 23 zeigt eine Struktur für DaaS (Data as a Service) anhand von Patientendaten. Das Modell ist Übertragbar auf Finanz-, Versicherung-, und andere Industriezweige für welche Muster und Mustererkennung als Basis für Prädiktion brauchen und verwenden.

Fig. 24 zeigt, wie basierend auf der Zustimmung von Patienten und/oder basierend auf der Registrierung von Patienten, Ärzte und R&Ds beim Trust Center/AA-Agentur, die Content-Daten (z.B. prä-, klinische und Forschungsdaten und Resultate) entweder mit maskierten Identitäten rückverfolgbar für Patienten verwendet oder durch Entfernen der biometrischen Marker vollkommen anonym genutzt werden können.

Fig. 25 zeigt das FEDE Verfahren und System, das die Zusammenarbeit zwischen Ärzte und Spitzenforschung unter Wahrung von Privacy, Secrecy und Anonymity für personifizierte Medizin ermöglicht und vereinfacht.

Fig. 26 zeigt den Datenfluss und Prozess für den Aufbau von DaaS (Data as a Service) im Gesundheitswesen.

Fig. 27 zeigt eine beispielhafte Aufteilung des erwirtschafteten Gewinnes pro Datensatz unter den Beteiligten und Rückfluss eines Teils des Gewinns als Vergütung an Patienten und Datenlieferanten.

Detaillierte Beschreibung einer bevorzugten Ausführungsvariante

Figur 1 illustriert schematisch eine Architektur für eine mögliche Realisierung einer Ausführungsvariante des biometrischen, insbesondere fingerprint-basierten, Encryption-Decryption Engine zur kontrollierten Handhabung und gesicherten Übertragung personifizierter, sensibler Daten, falls dafür ein mobiles Gerät modifiziert werden muss. Allfällige gesetzliche Vorschriften zur Privacy und Secrecy der Patientendaten lassen sich z.B. dadurch begegnen, dass ein Patient/Consumer/Originator entweder mit der Unterschrift seine (Patienten)-Zustimmung gibt und/oder Registrieren der Consumer-IDs, im konkreten Beispiel die MED_ID, mit welchem Confidant und/oder Gruppe von Personen, wie z.B. Research & Development, Finanz-, Versicherungswesen, Intelligence, Anwälte, usw. sensiblen Daten austauscht und zur Verfügung gibt, d.h. z.B. zwei verschiedene Abdrücke von je einem Finger aus je einer Hand elektronisch erfassen zu lässt. Ein Fingerabdruck der einen

Hand gilt für die Authentifizierung. Der zweite Fingerabdruck wird für die Autorisierung verwendet.

An der Quelle respektive Quellen und im ganzen Lebens-, und Transportzyklus der sensiblen Daten sind die Personenbezogenen Daten von den Daten, welche den Inhalt der Mitteilung beschreiben, also prä-, klinischen, Labor-, Finanz-, Versicherungs-, Intelligence Daten strikt getrennt. Das erfindungsgemässe System und Verfahren kann auf alle Arten von persönlichen, biometrisch gewonnenen Messungen angewendet werden, denn es als Core der Erfindung werden zwei unabhängige zufällig generierten, persönlichen Schlüssel bestimmt, womit alle Arten von Daten, wie z.B. Video, Sprachaufzeichnungen, Bilder, Texte u.v.n.m. mit (a) einem persönlichen, biometrischen Schlüssel verschlüsselt werden und (b)die Daten mit dem zweiten, unabhängig vom ersten Schlüssel, zufällig generierten, persönlichen Schlüssel markiert werden.

Die Applikation oder APP (siehe Fig. 1) enthält verschiedene Funktionalitäten, trennt Daten nach Sensitivität, Bezug, Prozesse und Informationsfluss. Das erfindungsgemässe System und Verfahren ist skalierbar für End-Nutzer-spezifische Erweiterungen, responsive und besteht aus mindestens folgenden Teilen, damit Das erfindungsgemässe System und Verfahren wirken können:

1. Person-bezogene Informationen sind immer streng vom Inhalt der Daten getrennt.
2. Erste Hilfe Informationen oder bestimmte Informationen und/oder Massnahmen zu einem Geschäftsfall mit hoch-sensitiven Datentransfer.
3. Liste der Referenz-Personen z.B. Arzt, Apotheker, aber auch Treuhändler, Anwalt für die respektive für den die Daten bestimmt sind.
4. Ein SOS-Symbol, im Fall von Patienten, womit die SOS-Prozedur ausgelöst wird.
5. CRUD-Right Administration, womit Eigentümer eines End-Nutzer-Gerätes und der Daten die Hoheit aller dezentral gespeicherten Daten besitzen und die Zugriffsrechte auf Content-Daten und personenspezifische Daten (Dokumente/Daten) für die Referenz- Personen zeit-, und ortsunabhängig eigenständig bestimmen und verwalten.

Wie die Fig. 8 a/b illustrieren, kann die Applikation oder APP verschiedene Funktionalitäten enthalten, insbesondere kann sie die Daten nach Sensitivität, Bezug, Prozesse und Informationsfluss trennen. Die App kann z.B. skalierbar für End-Nutzer-spezifische Erweiterungen realisiert sein. Die Person-bezogenen Informationen enthalten Felder, wie Namen, Vornamen, usw. (vgl. Fig. 12). Teile dieser Felder oder alle Felder werden genutzt, um die beiden pseudo-persönlichen, biometrischen Schlüssel Autorisierungsschlüssel und Authentifizierungsschlüssel, zu bilden. Diese Felder oder Teile davon können insbesondere dazu verwendet werden, über die gängigen, elektronischen Übermittlungsarten, wie Bluetooth, infrared, scanning, elektronische Visitenkarte an „Consumer", zu übertragen. Der damit generierte pseudo-persönliche Autorisierungs-Schlüssel kann vom Gerät-End-Nutzer auch als elektronische, authentische Unterschrift verwendet werden. Die Liste für „*Erste Hilfe oder Informationen über zu treffenden Massnahmen*" kann in Zusammenhang mit der „*SOS-Funktionalität*" wichtig sein, wenn ein End-Nutzer eines Gerätes bewusstlos ist. Helfer/Notarzt können z.B. damit lebenswichtigen Informationen zur bewusstlosen Person erhalten, wie z. B. Allergien, wichtige Medikamente und ihre Verabreichung, zu benachrichtigende Person, u.v.n.m. Für andere Fälle, wie Finanz-, und/oder Versicherungs-, und/oder Fälle, wo die Sensitivität der Daten hoch ist, lassen sich in diesen Felder auch z.B. Instruktionen technisch erfassen, wie Benachrichtigung, Umgang mit den Daten, Alert-Auslöser, z.B. im Fall von Intelligence.

Die Liste referenzierter Personen kann z.B. umfassen (a) im Fall von Patientendaten die Felder MED[1,2,..]-ID, Apotheker[1,2]-ID, allgemein die Bezugsperson-ID eines Gesundheits-Leistungserbringers und/oder die R_D_-ID (ID von Research and Development, Labors, ...). Für andere Fälle, wie z.B. Finanz-, und/oder Versicherungs-, und/oder Fälle, wo die Sensitivität der Daten hoch ist, umfasst sie die genaue Referenz-ID der Person, für welche die Daten bestimmt sind. Als persönliche Erweiterungsmöglichkeiten kann z.B. dem Eigentümer des End-Nutzer-Gerätes die Möglichkeit angeboten werden, das erfindungsgemässe System und Verfahren für die Autorisierung/Authentisierung mittels pseudo-persönlichen, biometrischen Messungen Zugriff auch auf anderen, sensitiven Daten anzuwenden, z. B. um online Finanztransaktionen zu tätigen u.v.n.m. Das erfindungsgemässe System und Verfahren lässt sich in beliebigen technischen Gebieten anwenden, weil die kleinste Einheit, d.h. die im Transfer der hoch-sensitiven Daten einbezogene Subjekte, immer aus „Producer-Eigentümer-Sender" – „Consumer-Berechtigter-Receiver" und der AA-Agency besteht,

welche als unabhängige, Drehscheibe, im Sinne einer Trust-Plattform, zwischen den beteiligten Subjekten „Producer-Eigentümer-Sender“ – „Consumer-Berechtigten-Receiver“ wirkt.

Für die AA-Agencies kann es z.B. vorteilhaft sein, eine Domain-Name-Konvention einzuführen, womit die AA-Agencies untereinander sicher kommunizieren können. Beispielsweise kann die Nomenklatur für Domain-Name wie folgt definiert ein: <frei_wählbare_Bezeichnung>.<landesspezische_grobe_unterteilung>.<land>, also zum Beispiel <frei_wählbare_Bezeichnung> - meineAA-AgenturNPU; <landesspezische_grobe_unterteilung> - bs; <land> - ch, oder <frei_wählbare_Bezeichnung> - monAA-Service; <landesspezische_grobe_unterteilung> - Alsace; <land> - fr. Die AA-Agency kann z.B. für jedes Individuum Metadaten, Schlüssel, Zugriffsrechte, URIs, Verfahren, Regeln, Regelwerke speichern und verwalten, und ob und wie Daten zwischen den beteiligten Subjekten „Producer-Eigentümer-Sender“ – „Consumer-Berechtigten-Receiver“ ausgetauscht werden müssen respektive dürfen. „Producer-Consumer“ müssen vorgängig den Austausch zustimmen oder der „Consumer“ vom „Producer-Eigentümer-Sender“ vorgängig bestimmt werden. Der „Producer-Eigentümer-Sender“ kann z.B. für die berechtigten, zugeordneten registrierten „Consumer(s)-Berechtigte(n)-Receiver(s)“ aktiv die Granularität der Zugriffe für jedes Dokument und für jeden „Consumer-Berechtigten-Receiver“ bestimmen müssen, einstellen, verwalten und/oder gewähren müssen.

In der Ausführungsvariante mit der SOS-oder Alarm-Funktion kann ein Helfer der Zugriff auf Content-Daten des Gerätes eines Bewusstlosen braucht um lebenswichtige Informationen zum bewusstlosen Eigentümer des End-Nutzer-Gerätes zu erhalten. Mit dem Betätigen der SOS- oder Alarm Funktion ist das End-Nutzer-Gerät automatisch und per sofort mit einer offiziellen, beglaubigten Alarmzentrale im jeweiligen Aufenthaltsland verbunden, welche die SOS-Alarm-Funktionalität automatisch anfordert und in der APP anbindet. Der Zugriff auf die persönlichen Daten, die verschlüsselt lokal auf dem Benutzergerät gespeichert sind, ist Dritten, welche die SOS-Funktion betätigen, nur dann möglich, wenn diese Dritten von der Alarmzentrale authentifiziert worden sind. Die Alarmzentrale gewährt Zugriff auf das End-Nutzer-Gerät der bewusstlosen Person und schaltet die entsprechenden Content-Daten zur bewusstlosen Person frei. Die Verbindung zwischen Alarmzentrale und End-Gerät der bewusstlosen Person kann z.B. mit dem Betätigen der SOS-Funktion automatisch erstellt

werden. Dritten können die eingeleiteten Massnahmen, Entscheide u.v.n.m. erfassen. Beim Senden der Daten bettet sich, der biometrisch generierte Autorisierungschlüssel der bewusstlosen Person zusammen mit den Daten des Helfers im Daten-Paket ein und wird mit dem zweiten biometrischen Schlüssel der bewusstlosen Person verschlüsselt. Das Trusted Center kann dabei z.B. die Notfall-Prozedur und sämtliche Content-Daten aufgrund des Autorisierungschlüssel der bewusstlosen Person erfassen. Notärzte, Gesundheitsfachpersonen oder solche, welche ein End-Nutzer-Gerät mit derselben APP besitzen, können das eigene Gerät für die Identifikation gegenüber dem Trusted Zentrum z.B. mittels gängigen Verfahren (z.B. Bluetooth, infrared, scanning, WiFi, etc.) die Notfall-Prozedur vom Gerät der bewusstlosen Person anstossen, um auf die Content-Daten der bewusstlosen Person zugreifen zu können und die angewendeten Massnahmen, Entscheide in das Notfall-Dossier der betroffenen Person einzutragen zu können. Das Gerät der bewusstlosen Person bettet den biometrischen, pseudo-persönlichen Autorisierungsschlüssel sowohl der betroffenen, bewusstlosen Person als auch der helfenden Dritten/Notarzt/Gesundheitsfachperson in die Notfall-Record-Daten ein und verknüpft die persönlichen Daten des Notarztes/Gesundheitsfachperson/… mit denen des bewusstlosen Eigentümers des End-Gerätes.

Die Datenhoheit verwalten Eigentümer eines End-Nutz-Gerätes und Dateneigentümer mit den CRUD (C(reate), R(ead), U(pdate), D(elete)) Rechten lokal auf dem End-Nutzer-Gerät. Nur ein Gerät-, und Daten-Eigentümer darf die CRUD-Zugriffsrechte auf die Dokumente an „Consumer-Berechtigen-Receiver“, wie z.B. MED_[1,2,..], zeit-, und/oder ortsunabhängig vergeben, verwalten und darüber verfügen. Fig. 9 zeigt ein Beispiel für CRUD Zugriff angewendet auf Dokument 1 und 2. MED 1 welche z.B. Leserecht (R) für Dokument 1 und Nachführrecht (U= update) auf Dokument 2 erhalten. MED 2 kann z.B. erstellrecht (C=create) Recht für Dokument 2 erhalten, d.h. kein Zugriffsrecht für Dokument 1 usw. Die Bezeichnung MED_[1,2,..] soll als konkretes Beispiel für den Fall von Patientendaten stellvertretend für alle mit einer eindeutigen ID gekennzeichneten und nur genau auf die Person bezogene, eindeutige Kennzeichnung dienen. Mit der ID-Kennzeichnung, z. B. MED[1], bildet ein End-Nutzer und Eigentümer „Producer“ eines Gerätes und Daten eine direkte Verbindung zum „Consumer“ und Inhaber der ID-Kennzeichnung, im Beispiel MED[1].

Die Dokument[1,2,...]-Namen können z.B. in der Maske der Applikation eines End-Nutzers-Gerätes im Klartext dargestellt werden. Der Dokumentname kann dabei ein Teil der gesamten, absoluten Adressierung, somit des physikalischen Speicherortes eines Dokumentes, sein. Dieser kann z.B. mittels URI (Unique Resource Identifyer) eines jeden Dokumentes eineindeutig festgelegt sein, also die direkte, Adressierung des Speicherortes eines Dokumentes, im Sinne von RFC 3986. Speicherort und Dokumentnamen und die dazugehörigen Ressourcen (Content-Daten) sind als Metadata (a) dem „Producer-Eigentümer-Sender" eindeutig zugeordnet und (b) als Metadata in der AA-Agentur, d.h. dem Trust-Center, mit dem pseudo-persönlichen, biometrischen Authentizierungs-Schlüssel verschlüsselt, gespeichert. Dokumente und/oder URIs (Uniform Resource Identifier) werden in der AA-Agency vor dem Senden an den „Consumer" mit dem Authentizierungs-Schlüssel des Producers entschlüsselt und dann mit dem zweiten, pseudo-persönlichen, biometrischen Authentizierungs-Schlüssel des „Consumers" verschlüsselt. Wie gezeigt, ist die Kenn-ID wie MED_[1,2,...] durch andere ebenso eindeutige Kenn-Ids ersetzbar. Verfahren und System dieser Lösung können auf andere technischen Gebiete, wie Finanz,- Versicherungswesen, Intelligence-Technologie u.v.n.m. angewendet werden, wenn es darum geht, hoch sensitiven Daten an Dritten und/oder von Dritten an Gruppen zu senden, und/oder Maschine-zu-Maschine, automatische Mustererkennungen durch künstliche Intelligenz, machine- oder deep learning zu senden. Sensitive Daten können so von der Identität des Urheber maskiert analysiert oder verarbeitet werden, wobei jedoch die Identität des betroffenen Individuums oder der zugeordneten Referenz-Person geschützt/geheim bleibt, und so Privacy, Secrecy und Anonymity des Individuums oder der Referenz-Person erhalten bleibt.

Mit FPC-Sensoren und entsprechender Integration beim mobilen Geräte können z.B. persönliche Fingerprints erfasst werden. FPC (Fingerprint Cards) könne die volle Breite von biometrischen Technologien erfassten, insbesondere Fingerprint Sensors, biometrische Processoren (basierend auf spezialisierten Algorithmen) und Fingerprint Sensor Moduls (Sensor integriert in den Processor. Im Stand der Technik gibt es hochwertige Sensoren für Gesichtserkennung oder Iris, Retina-Scanning, Spracherkennung, Erkennung der Handfläche-Geometrie, usw. Wichtig ist, dass jede biometrische Messung (Fingerprint, Gesichtserkennung oder Teile des Gesichtes, Iris, ...) auf Sensor-Ebene eine Bit-Sequenz von „1" und „0" ergibt. Prozesse und intelligente Softwares rekonstruieren aus den Bitfolgen „1" und „0" eineindeutig Fingerprints,

Gesichter oder Teile davon usw. Erfindungsgemäss kann die Bit-Folge (Repräsentation) der persönlichen, biometrischen Eigenschaften von Körperteilen selbst vor dem Eigentümer eines End-Gerätes geschützt bleiben, indem die erzeugten, pseudo-persönlichen Schlüssel geschützt und verborgen erzeugt werden. Die echten, Bitsequenzen von gescannten Körperteilen werden zusätzlich innerhalb des Gerätes separat und zugriffssicher gespeichert. Die persönlichen, zufällig generierten, biometrischen Schlüssel, werden vom automatisierten Trust-Center oder Trust-Einheit verwendet, um die Identität eines End-Nutzers zu validieren und verifizieren. Beispiel für eine Bit-Sequenz für den Abgriff der beiden Fingerprints wird in Fig. 10 gezeigt, im Speziellen für zwei verschiedene Fingerprints, welche verschieden Lang sein können. Z.B. stellen „Touch ID"-fähigen Geräte automatisch fest, ob ein Sensor vorhanden ist, um die persönliche, biometrische Messung zu erfassen. Fig. 11 zeigt weiter ein mögliches Verfahren zur Erzeugung der pseudo-persönlichen-Codes.

Für die Lösungsvariante sind höchstens zwei Fehler bei der Anmeldung erlaubt. Bei Fehler wird die Funktionalität der Applikation im End-Nutzer-Gerät für die Übertragung von sensitiven Daten blockiert. Dadurch können mehrfache, trial and error Versuche verhindert werden, z.B. um den Zugriff auf die Applikation im End-Gerät zu hacken.

Fig. 12 zeigt beispielshaft die Feldnamen und minimale Anzahl der Felder für Standard-Informationen. Zu den Pflichtfelder können die weltweit eindeutige Pass-, oder ID-Nummer, und eine länderspezifsche ID, oder in der Schweiz die AHV-Nummer zählen. Ein Verfahren übersetzt den Wert eines Textes in Binary-Repräsentation um, eine Folge von „1" und „0", womit eine individuelle, biometrische Messung auch zu randomisiert werden kann. Fig. 13 zeigt den Binary Code für jeden Text-Code aus Fig. 10. Beispielsweise entspricht „Nunzio" dem Binary-Code „01001110 01110101 01101110 01111010 01101001 01101111" oder Pass-ID „AA3480011" entspricht dem Binary-Code „01000001 01000001 00110011 00110100 00111000 00110000 00110000 00110001 00110001" usw. Ein Verfahren („generatePseudoPersonalizedKeyOne") kann z.B. eindeutige, individualisierte, randomized Schlüssel erzeugen, z.B. indem ein End-Nutzer des Gerätes aufgefordert wird, eine Sequenz von Zahlen zwischen null und neun (0..9) in beliebiger Reihenfolge ohne Wiederholung zu tippen. Wenn ein End-Nutzer eine der Zahlen (0..9) eintippt, welche bereits verwendet ist, fordert der Algorithmus ihn auf,

stattdessen eine neue Zahl anzugeben oder schlägt als Wahl eine Zahl aus der Liste der noch nicht verwendeten Ziffern vor. Kontinuierlich, stetig aufsteigende, also null bis neun, oder kontinuierlich, stetig absteigende, also neun bis null, Ziffer-Folgen verwirft der Algorithmus und gibt dem End-Nutzer Vorschläge an. Fig. 14 illustriert die Eingabe eines End-Nutzer mit einer zufällige Folge [4,9,0,7,6,5,2,1,8,3]. Damit werden den Werten in der Spalte „Feld-Namen" die Bit-Sequenzen aus den zufällig zugewiesen Felder zugeordnet: (0,4), (1,9), ...(9,3). Im Beispiel „Nunzio" erhält die Bit-Sequenz der Pass-ID „01000001 01000001 00110011 00110100 00111000 00110000 00110000 00110001 00110001". Die Nationalität „It" erhält die Bit-Sequenz des Geburtstages „00110001 00110010 00101110 00110111 00101110 00110001 00111001 00110101 00111001" usw. Alle zehn Bit-Sequenz-Felder und die erste echte, persönliche biometrische Messung,

Um die zwei persönlichen, randomized Schlüssel zu erzeugen, kann die Zielfunktion z.B. zufällig Bit-Operationen (Addition, Subtraktion, Division, Multiplikation) oder boolesche Operationen (AND, OR, XOR) auf die Bit-Sequenz-Folgen anwenden. Der damit erzeugten Schlüssel kann z.B. mindestens aus 512 Bits bestehen. Die temporär gespeicherte Zahlenfolge [4,9,0,7,6,5,2,1,8,3] kann z.B. mit dem generierten Autorisierungs- Schlüssel encrypted werden, im End-Gerät gespeichert und die im Klartext gespeicherte Sequenz [4,9,0,7,6,5,2,1,8,3] zu einem späteren Zeitpunkt, gelöscht werden. Bei Bedarf lässt sich die ursprüngliche Zahlenfolge ermitteln. Dieser erste Schlüssel, als Autorisierungsschlüssel, wird hier als FP1 referenziert, um am Beispiel der Fingerprints, das erfindungsgemässe Verfahren und System zu illustrieren. Der Schlüssel FP1, kann aus der Verknüpfung einer persönlichen, biometrischen Messung, in diesem Fall Fingerprint eins, und einer Vertauschung, der als Binary-Code dargestellten Werte der Feld-Namen, erzeugt werden.

Implementierte Verfahrensschritte (im Folgenden „startDialogForFingerPrintTwo") können z.B. den Dialog mit einem End-Nutzer durchführen, um, im Beispiel mit Patientendaten, den zweiten Fingerprint für die Verschlüsselung der Content-Daten (Informationen, Daten, Dokument) zu verwenden. Dieser zweite Schlüssel wird also als zweite Bitsequenz der persönlichen, biometrischen Messung erfasst und erzeugt, mittels welchem die Inhaltsbezogenen Daten (anonymisierte und/oder maskierte Content-Daten) verschlüsselt werden (hier als Autorisierungsschlüssel/Autorisierung referenziert). Der erste Schlüssel (Authentisierungsschlüssel) wird zur Verschlüsselung der personen-spezifischen Daten

(Authentisierung) verwendet, welche den mit dem zweiten Schlüssel verschlüsselten anonymisierte und/oder maskierte Content-Daten zugeordnet sind. Zu den bereits in den Paragraphen zur Generierung des ersten Schlüssels erläuterten Schrittfolgen, können die Verfahrensschritte „generatePseudoPersonalizedKeyTwo“ vom End-Nutzer eine zweite Zahl-Folge, z.B. [5,9,1,8,3,4,6,2,7,3], verlangen. Diese sollte verschieden sein von der ersten Zahlenfolge [4,9,0,7,6,5,2,1,8,3], welche für die erste biometrische Messung, z.B. Fingerprint eins, verwendet wurde. Zusätzlich, kann das Verfahren verifizieren und validieren, ob der zweite, zufällig generierte, pseudo-persönlicher Schlüssel (FP2) vom ersten Schlüssel FP1 verschieden ist, und z.B. nicht aus 000…000 oder 1111…1111 Folge Bits besteht. Die zweite Zahlenfolge [5,9,1,8,3,4,6,2,7,3] wird mit dem Authentifizierungschlüssel FP2 verschlüsselt im End-Nutzer-Gerät gespeichert. In der Folge können die beiden im Klartext gespeicherten Zahlenfolgen [4,9,0,7,6,5,2,1,8,3] und [5,9,1,8,3,4,6,2,7,3] gelöscht werden.

Mit dem erfindungsgemässen Verfahren und System kann somit: (1) aus den Bit-Sequenzen der persönlichen, biometrischen Messungen von Körperteilen zufällig erzeugte pseudo-persönliche Schlüssel erzeugen; (2) Privacy, Secrecy und Anonymity eines Individuums gewährleisten, weil die echten persönlichen, biometrischen Messungen nur im Gerät des Eigentümers sicher gespeichert werden und nicht aus dem Gerät gesendet werden; (3) eines der zwei unabhängig, zufällig generierte, pseudo-persönlicher Schlüssel verwenden, um die Identität einen End-Nutzer mit dem Autorisierungsschlüssel zu maskieren. Der Autorisierungsschlüssel dient als Marker und wird in Dokumente, Informationen aller Daten automatisch eingebettet. Der zweite unabhängig, zufällig generierte, pseudo-persönlicher Schlüssel, der Authentifikationsschlüssel, dient um die sensitiven Daten (referenziert als Content-Daten) aller Art zu encrypten und zu decrypten; (4) Für die Encryption-Decryption werden zwei verschiedene der bereits etablierten Algorithmen eingesetzt. Erforderlich kann sein, dass die verwendeten Algorithmen für jede der beiden Aufgaben verschieden, robust, schnell und unbreakable sein; (5) für jeden ausgewählten Algorithmus genau eines der beiden zufällig generierte, persönliche pseudo-Schlüssel verwendet werden; (6) Der Confidant/Arzt/Research-Verantwortliche usw., der vom Producer/Originator in der Applikation aufgeführt ist, z.B. MED_[1], darf, aber muss nicht unbedingt in dergleichen AA-Agency/Trust Center registriert sein, denn aufgrund der Abbildung zwischen Originator-Confidant, wird in der AA-Agency, wo der Originator/Producer registriert ist

sowohl die Kenn_ID als auch der Link, wo der Consumer/Confidant registriert ist – also als Ressource – mit dem Autorisationsschlüssel des Originator/Producer gespeichert. Weil die AA-Agencies über Domain-Namen verbunden sind, können die AA-Agencies, solange z.B. technische Randbedingungen von Kredit-Karten-Zentren erfüllt sind, auch weltweit verteilt sein.

Fig. 15 illustriert ein Algorithmus für das Erstellen von zwei unabhängige, Random-generierten, pseudo-persönlichen Schlüssel. Als Variante kann ein Selbst-Zerstör-Mechanismus den End-Nutzer vor Angriffen schützen. Falls z.B. Hersteller von Geräten die wahren Bit-Folgen aus den echten, persönlichen, biometrischen Messungen, z.B. Finger-Prints, nicht an zwei verschiedenen Speicherorten im Device/Gerät eines End-Nutzers speichert, kann das Verfahren die getrennte Speicherung der beiden echten, persönlichen, biometrischen Messungen vornehmen. Das Verfahren und System kann z.B. garantieren, dass falls ein Eindringling versucht in eines der beiden oder beide Speicherorte, wo im Device die biometrischen Messungen und/oder eines der beiden Speicherorte im End-Nutzer Device und wo die zufällig generierten pseudo-persönlichen Schlüssel aufbewahrt sind, einzudringen, ein Selbst-Zerstör-Mechanismus eingreift, welcher beide zufällig generierte pseudo-persönliche Schlüssel löscht, im Beispiel FP1 und FP2, und die Funktionalität der Applikation im End-Nutzer-Gerät für den Datentransfer blockiert. Um erneut das System benutzen zu können, muss ein End-Nutzer dann die Schritte zur Generierung der beiden Schlüssel, also Autorisierungschlüssel und Authentizierungsschlüssel (FP1/FP2), wiederholen. Die Wiederherstellung der beiden Schlüssel, also Autorisierungschlüssel und Authentizierungsschlüssel, kann z.B. als Variante nur dann möglich sein, dies um die AA-Agencies vor Angriffen zu schützen, wenn ein End-Nutzer sich bei einer beglaubigten Person ausweist. Ein End-Nutzer muss sich z.B. mit einem amtlich anerkannten Dokument, Pass oder ID, bei der beglaubigten Person ausweisen. Die beglaubigte Person kann sich beim Trust-Center, i.e. der AA-Agency, mit seinen zufällig generierten pseudo-persönlichen Autorisierungschlüssel (FP1) anmelden, und Autorisierungschlüssel und Authentizierungsschlüssel des verifizierten End-Nutzers terminieren (FP1/FP2), welcher die Autorisierungschlüssel und Authentizierungsschlüssel neu erstellen muss. Die im Trust Center bzw. in der AA-Agency terminierten Schlüssel können z.B. nur logisch terminiert werden, jedoch nie physikalisch gelöscht werden. Damit ist im Haftungsfall die Historie der Schlüssel aus den Zeitstempeln und Aktivitäten auf die Schlüssel (z.B.

gelöscht, weil Gerät kompromittiert, am Tag,... Monat ... Jahr ... um ... Uhr ... Minuten ...; neu erstellt ... beglaubigte Person FP1 der beglaubigten Person) erhalten und lückenlos rückverfolgbar.

Der Autorisation-Authentication-Mechanismus kann z.B. auf zwei Arten geschützt werden:

(1) Cross-Over-Mechanismus: Bei einem Refresh-, Wiederbestimmungsprozess eines End-Nutzers werden im Zweifelsfall die Authentisierung und die Autorisierung eines End-Nutzers verifiziert und validiert. Dieser Fall kann z.B. dann eintreten, wenn mit einem Hackerangriff, wie MITM (man-in-the-middle), session-hijaking, session-rerouting, XSS (cross-site-scripting), sql-injection und/oder andere, weitere Hacker-Angriffe, Gefahr besteht, dass Eindringlinge die End-Nutzer-Identität stehlen könnten. Diese Lösung wirkt präventiv, daher wird ein Cross-Over- und Refresh-Mechanismus eingesetzt. In unvorhersehbaren, zeitlichen Abständen, wird ein End-Nutzer-Gerät aufgefordert die Identität mit der AA-Agency zu verifizieren und zu validieren. Das Trust Center erfragt von einem End-Nutzer den Finger-Print für die Autorisierung zu transferieren. In der Trust Center (AA-Agency) Datenbank wird der erfragte Finger-Print mit dem Authentizierungs-Fingerprint verglichen. Mutatis mutandis gilt es dies für den zweiten Finger-Print, deshalb „cross-over". Das Testverfahren dient dazu, zu einem nicht vorhersagbaren Zeitpunkt, die pseudo-persönlichen Schlüssel in End-Nutzer-Gerät und in der AA-Agency zu vergleichen. Der ad hoc Abgriff der persönlichen, biometrischen Daten (Fingerprints, Gesichtserkennung, ...) dient lediglich als Auslöser, um auf dem End-Nutzer-Gerät mit den anfänglich bereits gespeicherten, echten, persönlichen biometrischen Bit-Sequenzen und die Bit-Sequenzen der mit den Random-generierten Zahl-Folgen die beiden Schlüssel zu überprüfen. Ein Vorteil ist dabei, dass, falls ein Eindringling sich eines End-Nutzer Gerätes ermächtigt und sich den Zugang zur Datentransfer-Applikation verschafft hat, er bei der ad-hoc Erzeugung der beiden zufällig generierten, pseudo-persönlichen Schlüssel fehlschlagen wird. Somit kann der AA-Agency Server mit hoher Sicherheit schliessen, ob es sich um den echten End-Nutzer des Gerätes oder um einen Eindringling handelt. Im zweiten Fall kann z.B. das Trust Center die Session schliessen und die Funktionalität des Datentransfers auf dem End-Gerät unmittelbar blockieren.

(2) Schliess-Mechanismus: Jedes Mal, wenn der pseudo-Finger-Print lokal im End-Nutzer-Gerät „on the fly" oder ad hoc generiert wird, wird die Netz-Verbindung unterbrochen. Der Zeitunterbruch ist minim und nur solange, bis der jeweilige Schlüssel, also Autorisierungsschlüssel und/oder Authentisierungsschlüssel, erzeugt wurde. Danach verbindet und synchronisiert sich das End-Nutzer-Gerät automatisch mit dem Netz. Mit dieser Massnahme kann z.B. eingeschleuste Malware bei der Erzeugung der Schlüssel umgangen werden, weil das Verfahren, welche auf die lokal auf dem End-Nutzer-Gerät gespeicherten Daten zugreift, nur auf die Felder zugreifen kann, die vorgängig bestimmt wurden.

Der Sende-Mechanismus kann am Beispiel von sensitiven Patientendaten illustriert werden: (1) Alle Person-bezogenen Daten aus „Person-bezogene Information" (vgl. Fig. 8 a/b), können z.B. mit dem Verfahren automatisch durch den pseudo-persönlichen Schlüssel, wie z.B. Fingerprint PFP(1) (Autorisierungschlüssel), ersetzt werden. Die Person-bezogene Information und/oder weitere definierbare Individuums-relevanten Daten oder Daten, die es erlauben, exakt auf die Identität einer Person zu schliessen, werden beim eigentlichen Datentransfer nicht übermittelt oder mit den Daten (Content-Daten), welche Inhalte beschreiben, vermischt; (2) Der erzeugte PFP(1) (Pseudo-Fingerprint) markiert die inhaltbezogenen Daten, wie prä-, klinischen-, Labordaten, Bilder, usw. im gesamten Lebenszyklus eines Transfers der Daten, welche frei sind von Person-bezogenen Daten, in welche das Verfahren den Autorisierungsschlüssel einbindet und einbettet; (3) Die MED-IDs der Bezugsperson (MED1, ... MEDs) werden mit dem Autorisierungsschlüssel PFP(1) (Pseudo-Fingerprint) verschlüsselt; (4) Das versandbereite Protokoll an die AA-Agentur kann somit enthalten: (i) den Random-erzeugte pseudo-persönliche Schlüssel PFP(1), (ii) mit PFP(1) verschlüsselte Referenz-Peron, z.B. MED-ID_n, (iii) mit PFP(2) ≠ PFP(1) verschlüsselt Daten/Dokumente aller Art; (5) Im Trust-Center/AA-Agency werden Autorisierungs-, und Authentifizierungs-Schlüssel der beteiligten, dem Sender zugeordneten Medical-, und/oder R_D_IDs (Research and Development, Labors, ...) und die mit den jeweiligen Schlüssel verschlüsselten URIs (Uniform Resource Identifier (absolute Links zu den Dokumenten und Ressourcen)) der jeweiligen Patienten-Dossiers verwaltet; (6) Die eigentlichen, elektronischen Patienten-Dossiers befinden sich physisch an verteilten, dezentralen Speicherorten (vgl. Fig. 16), wo dieselben mit dem Authentikationsschlüssel eines Patienten verschlüsselt sind; (7) Die URIs der Content-Daten (i.e. Dokumente), also die Metadaten der elektronischen Content-Daten, sind encrypted und enthalten in der

encrypted URI den persönlichen Autorisations-Schlüssel PFP(1) eines Patienten. Sobald ein Patienten-Dokument durch Dritte geöffnet, verändert oder irgendwelche Aktivität damit vorgenommen wird, erhält ein Patient vom System automatisch eine Meldung. Jeder Schritt wird in der AA-Agency im Logbuch registriert und protokolliert. On–Demand und/oder ad hoc übermittelt das Trust Center die URIs von anderen elektronischen Dossiers bzw. Content-Daten von Patienten, basierend auf der vorgängig vergebenen CRUD-Rechte, an berechtigten Ärzten. So lässt sich on demand und ad hoc entweder das gesamte elektronische Patienten-Dossier (entspricht alle zu Consumer/Producer zugeordneten Content-Daten) oder ausgewählte Teile des elektronischen Patienten-Dossiers zusammenfügen. Das elektronische Patienten-Dossier und die zugehörige Identität eines Patienten kann im Klar-Text nur von einem, durch den Patienten berechtigten Arzt, gelesen werden. Mit dieser Methode kann die lokal beim Arzt installierte Software ebenfalls lokal beim Arzt die zwei asynchron erfassten Datenpakete, d.h. sowohl die Content-Daten (i.e. Dokument mit den klinischen Daten), als auch das Dokument mit der Identität eines Patienten (Authentisierung) zusammengefügt werden. Das System und Verfahren überprüft zuerst lokal beim Arzt, dass die separat gesendeten Autorisationsschlüssel PFP(1) eines Patienten , einmal angehängt an das Paket mit den klinischen Daten, ein zweites Mal angehängt an das Paket mit den Person-bezogenen Daten, identisch sind. Bei Übereinstimmung der beiden separat und asynchron gesendeten Autorisierungsschlüssel PFP(1) eines Patienten/Patientin, entschlüsselt das Verfahren mit dem Authentifizierungschlüssel MPFP(2) des Arztes beide Dokumente, welche streng getrennte Daten-Sorten (Person-bezogen/klinische Daten) beinhalten. Im Fehlerfall, d.h. falls mindestens eines der beiden Autorisierungschlüssel PFP(1) eines Patienten mit mindestens einem der separat gesendeten Autorisierungschlüssel PFP(1) eines Patienten nicht übereinstimme, dann bleiben beide Dokumente, also Person-bezogenes Datendokument und Dokument mit klinischen Daten, verschlüsselt. Das System und Verfahren vernichtet automatisch die beiden Dokumente. Der Teil der persönlichen Daten erscheint somit nur bei den berechtigten Ärzten. Selbst, wenn ein Eindringling das Klar-Text Dokument mit den klinischen Daten stehlen würde, würde er lediglich die klinischen Daten und den biometrischen Marker PFP(1) eines des Patienten verfügen. Umgekehrt, verhält sich gleich mit möglicherweise gestohlenen Person-bezogen Daten, denn darin ist kein Schlüssel irgendwelcher Art eingebettet. Ein Eindringling kann, beim Stehlen der klinischen Daten, nicht auf die exakte Person schliessen. Umgekehrt, beim Stehlen der Person-bezogene Daten kann ein Eindringling keine exakten, klinischen Daten

zuordnen. Weil die Abbildung zwischen den Autorisationsschlüssel, der als Biomarker PFP(1) in den Daten eingebettet ist und die realen Person-bezogenen Informationen ausschliesslich im Trust Center AA-Agentur stattfindet. Ein potentieller Hacker müsste für jedes Individuum die verschiedenen VPN-, Speicher-, und geheime Encryption ID Schlüssel erfolgreich hacken. Selbst bei Erfolg, hätte dann aber der potentielle Hacker entweder nur die klinischen Daten (Content Daten) ohne Bezug zur Person oder nur die Person-bezogenen Daten aber keine, zur Person eindeutig zugeordneten, klinischen Daten (Content Daten). Fig. 16 illustriert ein Beispiel einer Abbildung zwischen Patienten, zugeordneter Arzt oder Ärzte und Dokumente; (8) Das Trust Center/AA-Agentur dient bezüglich der Verschlüsselung der Daten wie eine „Relais- und Switch-Vorrichtung". Die jeweiligen zu übertragenden Daten und/oder Ressourcen-URIs, werden mit dem Authentifikationsschlüssel eines Senders/Producers/Eigentümers in der AA-Agentur entschlüsselt, dann unmittelbar mit dem Authentifikationsschlüssel des Receivers/Berechtigten/Consumers verschlüsselt; (9) Patienten haben zeit-, und ortsunabhängig Zugriff auf alle elektronischen Dossiers, welche eine eindeutige, verschlüsselte URI besitzen und im Trust Center gespeichert sind; (10) Das erfindungsgemässe System und Verfahren mit Encryption-Decryption von Content-Daten, hier klinischen Daten, welche Ärzte an verschiedensten in der ganzen Welt verteilten Research and Development (R&D) Unternehmen senden können, entspricht als Variante ebenfalls dem erfindungsgemässen System und Verfahren, wie zwischen Patienten/Ärzte jedoch mit dem wesentlichen Unterschied, dass das System und Verfahren den Ärzte nicht ermöglicht die Person-bezogenen Daten sowohl von Patienten als auch der Ärzte selbst in die an R&D gesendeten Fragen einzubetten. In dem Verfahren das Sende-Protokoll so ausgebildet, dass das an ein oder mehrere beim Trust Center/AA-Agentur angemeldeten und akkreditierten R&Ds usw. gesendeten Fragen, den Autorisationsschlüssel eines Patienten PFP(1) und den Autorisationsschlüssel des zugehörigen Arztes MPFP(1) enthalten/einbetten und die Fragen mit dem Authentifizierungsschlüssel R_D_i(FP2) verschlüsselt umfasst. Die Daten zu den Fragen an R&Ds sind, mutatis mutandis mit dem gleichen Verfahren wie zwischen Patient/Arzt den mit Authentifizierungsschlüssel R_D_i(FP2) des jeweiligen Verantwortlichen respektive der jeweiligen Verantwortlichen bei den verschiedenen R&Ds verschlüsselt; (11) Sobald die Fragen bei den R&Ds mit dem eigenen lokal gespeicherten Authentizierungsschlüssel R_D_i(FP2) des jeweiligen Verantwortlichen (dieses Verfahren eignet sich insbesondere für machine-to-machine Kommunikation, weil die Strings lediglich auf Identität verglichen werden müssen) entschlüsselt sind, kann der jeweilige Verantwortliche die

Problemstellung z.B. an mehrere Mitarbeiter übertragen. Die Identitäten sowohl des Patienten als auch des auftraggebenden Arztes bleiben in jedem Fall verborgen und maskiert/anonym und in Paar dem Autorisationsschlüssel des Patienten zugeordnet und dem Autorisationsschlüssel Arzt eindeutig aber eben maskiert, enthalten; (12) Die Antworten an den jeweiligen Arzt werden mit dem jeweiligen Authentifizierungsschlüssel R_D_i(FP2) verschlüsselt. Das Verfahren fügt im Sende-Protokoll zur AA-Agentur jeweils die Autorisationsschlüssel des Patienten PFP(1) und des Arztes MPFP(1) ein, welche der eindeutig gestellten Frage zugeordnet ist. In der AA-Agentur ermittelt das Verfahren den zum Arzt, also zu MPFP(1), zugehörigen Authentizierungsschlüssel MPFP(2) und die URIs wo R&Ds physisch die Antworten für den Arzt gespeichert haben. Danach setzt das Verfahren den umgekehrten Prozess an, um die Antwort eines Arztes an den betreffenden Patienten zu übermitteln.

Fig. 17 illustriert drei Schritte, um bestehende elektronische Patientendaten mit FEDE zu betreiben. Falls ein Patient beim ersten Arztbesuch keine MED_ID besitzt, dann registriert der Patient/die Patientin die MED_ID in die Applikation. Fig. 18 illustriert die Registrierung der MED_ID beim erstmaligen Arztbesuch. Fig. 19 illustriert den Prozess beim Arzt/Spital/Klinik, um Fragen an R&Ds unter Wahrung von Privacy, Secrecy und Anonymity zu stellen. Fig. 20 illustriert, dass die Metadaten zu den Dokumenten PD_[1..m] in Form von URL oder URI[1..q] im Trust Center/AA-Agentur gespeichert sind, genau mit Patienten-Autorisationsschlüssel P[1..r](FP1) markiert und P[1..r](FP2) verschlüsselt und genau einem Leistungserbringer MED_ID[1..t] zugewiesen. Die Dokumente können in eine Cloud, am besten in eine private Cloud gespeichert werden., Die URI eines Dokumentes ist eineindeutig.

Schliesslich wird die Identifikation bei R&Ds, Labors oder Gruppen von Beteiligten mit den folgenden Zeichnungen illustriert, insbesondere mit Fig. 21, die dem Zusammenhang und Abbildung zwischen MED_ID, Fragen von Ärzte an R&Ds und die Einbettung der Autorisation-Schlüssel von Patienten und Ärzte in die Fragen an R&Ds zeigt; Fig. 22, die den Decryption-Encryption-Decryption Mechanismen zur Wahrung von Privacy, Secrecy, Anonymity illustriert, um Fragen von Ärzten über bestimmte Patienten rückverfolgbar jedoch mit maskieren Identitäten der Patienten und Ärzten an beim Trust-Center/AA-Agency akkredierten Research und Development Laboratories zu senden; Fig. 24 , die basierend auf der Zustimmung von Patienten, die Registrierung von Patienten, Ärzte und R&Ds an die AA-Agentur illustriert, wobei die prä-, klinischen und

Forschungsdaten und Resultate entweder mit maskierten Identitäten rückverfolgbar für Patienten verwendet oder durch entfernen der biometrischen Marker vollkommen anonym genutzt werden können; und Fig. 25, die das FEDE Verfahren ermöglicht, wobei die Zusammenarbeit zwischen Ärzte und Spitzenforschung unter Wahrung von Privacy, Secrecy und Anonymity für personifizierte Medizin vereinfacht wird.

Mit DaaS (Data as a Service) können z.B. Patienten-Daten, welche von Ärzten mit der Zustimmung der Patienten an verschiedenen Research & Development Unternehmen/Labors/Pharma gesendet wurden, um aus Krankheitsbilder, Muster, Therapien usw. die für ein spezielles Individuum und für ein spezielles Krankheits-Bild optimale Therapie aus den grossen Datenmengen zu eruieren, sinnvoll verwendet werden, um Datenbanken und Entscheidungssystem zu bauen, und einem Krankheitsbild eine oder mehrere angewendeten Therapien, Nebeneffekte, toxikolische Untersuchungen/Auswirkungen usw., zu zuordnen. Somit, muss für Folgefälle von ähnlichen Krankheitsbilder-, und Muster nur eine Feinabstimmung auf bestimmte vorher mit Sicherheit eingegrenzte Muster durchgeführt werden. Für die zur Forschung und Entwicklung, Qualitätssicherung und weitere Zwecke verwendeten Datensätze kann z.B. eine Geldwerteinheit pro gelieferten Datensatz ausgehandelt werden. Fig. 27 illustriert eine Struktur für DaaS (Data as a Service), anhand von Patientendaten. Das Modell ist Übertragbar auf Finanz-, Versicherung-, und andere Industriezweige für welche Muster und Mustererkennung als Basis für Prädiktion brauchen und verwenden. Mit dieser Struktur können mehrere Erfordernisse unter Wahrung von Privacy, Secrecy und Anonymity erfüllt und realisiert werden: (1) Gesunde Individuen: Tagtäglich werden mittels elektronischen Geräten personen-spezifische Daten über die Funktionsweise von menschlichen Organe erfasst. Mit den beschriebenen Verfahren und Methoden können diese Daten entweder rückverfolgbar d.h. der Autorisierungsschlüssel PFP(1) der Daten-Sender, der z.B. mit dem Autorisierungsschlüssel MPF(1) eines zugeordneten Arztes unter Zustimmung eines Senders gekoppelt werden, können aber auch an Research und Development Zentren gesendet werden, z.B. für präventiv-Medizin, Epidemie-Vorbeugungen, Früherkennung, Korrelation von Mutationen auch in Funktion von Umweltfaktoren, Essgewohnheiten u.v.n.m. oder vollkommen anonym, d.h. die Autorisierungsschlüssel PFP(1) der Daten-Sender und/oder der z.B. persönliche Daten die mit dem Autorisierungsschlüssel MPF(1) eines zugeordnet Arztes unter Zustimmung

eines Senders gekoppelt sind, werden aus den Datensätzen gelöscht; (2) Chronisch Kranke und Individuen mit Seltenen Krankheiten: Das erfindungsgemässe Verfahren und System eignet sich insbesondere für chronisch kranke Individuen und/oder Individuen mit seltenen Krankheiten. Die Daten, welche mittels elektronischen Geräten und/oder kontinuierlichem Monitoring (Schrittzähler, Puls, Herz, Diabetes, ...) mit elektronischen Geräten erfasst werden, können direkt dem Arzt gesendet werden. Verfahren wie deep learning / artificial intelligence können aufgrund der kontinuierlich aus dem Monitoring erhaltenen Messdaten, Zeitreihenanalysen, Vergleiche, Muster erkennen und Veränderungen und/oder Mutationen von Mustern im Krankheitsbild aus den fast zeitnah (real-time) und synchron gesendeten Daten erkennen und je nach den, individuell in der jeweiligen Applikation eingestellten Parameter, Warnungen oder Alarm auslösen. Fig. 24 zeigt, wie basierend auf der Zustimmung von Patienten und die Registrierung von Patienten, Ärzte und R&Ds im Trust Center/AA-Agentur, die prä-, klinischen und Forschungsdaten und Resultate entweder mit maskierten Identitäten rückverfolgbar für Patienten verwendet können oder durch entfernen der biometrischen Marker vollkommen anonym genutzt werden können. Fig. 25 illustriert, dass das FEDE Verfahren die Zusammenarbeit zwischen Ärzte und Spitzenforschung unter Wahrung von Privacy, Secrecy und Anonymity für personifizierte Medizin auf eine neue Art ermöglicht und vereinfacht. Fig. 26 zeigt beispielhaft den Datenfluss und Prozesse für den Aufbau von DaaS (Data as a Service) im Gesundheitswesen zu Gunsten der personifizierte Medizin; (3) Der Anreiz für Individuen Daten zu liefern, kann z.B. darin besteht, dass für jede an Pharma, Research und Development oder Institutionen gelieferten Datensatz einen Geldwertbetrag, im Sinne von Angebot und Nachfrage, definiert wird, im Sinne einer Art balanced Datenbörse (vgl. Fig. 20, die eine Aufteilung des erwirtschafteten Gewinn pro Datensatz unter den assoziierten Beteiligten sowie einen mögliche Rückfluss eines Teils des Gewinns als Vergütung an Patienten und Datenlieferanten illustriert.)

Es ist noch einmal darauf hinzuweisen, dass die Verschlüsselung der persönlichen Daten erfindungsgemäss bereits an der Quelle erfolgt, also bevor die Daten transferiert werden. Eine AA-Agency (Autorisierung, Authentifizierung- Agency), wie z.B. Nexus, verwaltet beide biometrischen Schlüssel in einem dafür aufgesetzten Zugriffsserver. Die Daten können in diesem speziellen Zugriffsserver „transparent encrypted“ gespeichert sein, so dass selbst die Administratoren des Servers keine Möglichkeit haben auf diese Daten in irgendeiner Weise zu gelangen. Wie bereits

erwähnt, wird eine AA-Agency (Autorisierung, Authentifizierung- Agency) bevorzugt nach strengen Kriterien wie ein Kredit-Karten-Zentrum, wie z.B. Nexus, verwaltet werden. Alle gespeicherten Daten werden zusätzlich mit einem Schlüssel encrypted, der verschieden ist vom Autorisierungs- und Authentifizierungsschlüssel des jeweiligen verwalteten Individuums. Diese zusätzliche sog. „*transparent encrypted*" Massnahmen mit einem weiteren unabhängigen Schlüssel für bereits encrypted Ressourcen stellt ein weiterer Schutz für End-Nutzer dar, so dass selbst Administratoren des Servers keine Möglichkeit haben, auf die mit pseudo-persönlichen verschlüsselten Daten in irgendeiner Weise zuzugreifen.

Die Umrüstung eines Mobile-Gerätes für das erfindungsgemässe System und Verfahren kann z.B. in 6 Prozessschritten erfolgen:

Schritt 1: Umrüsten eines Mobilfunkgerätes, z.B. eines kommerziellen iPhones, zu einem persönlichen Smartphone für Originatoren, insbesondere Patienten, so dass es möglich ist, die Fingerprints von zwei verschiedenen Finger z. B. von je einer Hand in der lokalen iPhone-Card, wie beschrieben, zu registrieren. Ein Fingerprint P(FP1) wird für die Autorisierung, der zweite Fingerprint P(FP2) für die Authentifizierung P(FP2) verwendet. Der Fingerprint P(FP2) gilt als Verschlüsselung der Patientendaten. Beide Fingerprints sind bei einer AA-Agency hinterlegt (vgl. Fig. 1).

Schritt 2: Ein entsprechendes Modul, z.B. eine APP, führt Patienten durch alle notwendigen Schritte: Zusammenstellung, Validierung, Verschlüsselung und Transfer der Daten zum Vertrauensarzt (vgl. Fig. 2), wie beschrieben.

Schritt 3: Der Confidant, insbesondere ein Vertrauensarzt und/oder eine Learning Machine, entschlüsselt, wie beschrieben, die erhaltenen, reinen Patientendaten ohne Person-bezogenen Daten mittels der Learning Machine und/oder Deep Learning Machine und/oder AI (Artificial Intelligence/künstliche Intelligenz) - Module auf ein Individuum spezifisch festgelegten Parameter und überprüft die erhaltenen Daten auf Konsistenz und Qualität.

Als Ausführungsvariante können z.B. drei Triggerstufen detektiert werden: Grün, kein Handlungsbedarf; Gelb, Warnung; Rot, Alarmzustand (vgl. Fig. 4). Automatisch erstellt die Learning Machine auf Speichermedien, die vom Aussennetz

unzugänglich sind, ein Backup des Patientendossiers. Während des Backups trennt die Learning Machine den Arbeitsrechner des Vertrauensarztes vom Aussen-Netz. Sobald der Backup beendet ist, fügt die Learning Machine den Arbeitsrechner dem Netz wieder ein. Bei betrügerischem Datenzugriff z.B. mit darauffolgender, möglicher Erpressung, sind die gestohlenen Daten für Hakkers wertlos, weil die Zusammenhänge zwischen Person-bezogenen Daten und den Inhalt-beschreibenden Daten eines Individuums immer streng getrennt und gespeichert, zusätzlich verschieden verschlüsselt sind Falls Hackers die verschlüsselten Patientendaten mit einem Hakkers' Schlüssel sperren, kann der Vertrauensarzt jederzeit bis auf die zuletzt gespeicherten Daten vom Backup und/oder Ausfallsystem eine identische Kopie auf dem Hauptrechner installieren (lassen) und die von den Hackern verschlüsselten Daten bedenkenlos löschen.

Schritt 4: Der Confidant resp. Der Vertrauensarzt hinterlegt seine beiden Fingerprints M(FP1) Autorisierung zur und M(FP2) zur Authentifizierung ebenfalls bei einer vertrauenswürdigen AA-Agency (Authentifizierung und Autorisierung-Agency). Die maskierten, anonymisierten Patientendaten transferiert die Learning Machine oder der Confidant oder Vertrauensarzt mit dem erfindungsgemäss erweiterten Verfahren und System.

Schritt 5: Nur der Confidant bzw. Vertrauensarzt ist in der Lage, die mit maskierten Identitäten, verschlüsselten Patientendaten genau einem Patienten zu zuweisen und hat die volle Einsicht im Patientendossier, wie im Verfahren beschrieben.

Schritt 6: Forschungs-, und Entwicklungszentren verwenden die biometrisch maskierten Identitäten und verschlüsselten Patientendaten für die Korrelation zwischen Krankheits-Muster mit möglichen Medikamente, Therapien, Impfungen und für die Prävention von Epidemien. Als Rückmeldung erhalten nur Confidants, d.h. Vertrauensärzte, zu einem Krankheits-Muster die entsprechenden Empfehlungen verschlüsselt und Originator (Patient) bezogen, weil die Autorisierungs-Fingerprints M(FP1) und P(FP1) für ein Forschungs-, und Entwicklungszentrum zwar bekannt, jedoch anonym sind (vgl. Fig. 5 und 6).

Ansprüche

1. Biometrischer, fingerprint-basierter Encryption-Decryption Engine zur kontrollierten Handhabung und gesicherten Übertragung personifizierter, sensibler Daten, wobei mittels eines Mobilfunkgeräts biometrische Daten eines Originators erfasst werden und in einer SIM-Karte des Mobilfunkgerätes abgespeichert werden, dadurch gekennzeichnet,

dass zwei unterschiedliche Fingerprints (P-FP1/P-FP2) von zwei verschiedenen Fingern des Originators mittels des Mobilfunkgeräts erfasst und in der SIM-Karte des Mobilfunkgeräts dem Originator zugeordnet abgespeichert werden, wobei der erste Fingerprint (P-FP1) der Autorisierung und der zweite Fingerprint (P-FP2) der Authentisierung zugeordnet wird, und wobei der zweite Fingerprint (P-FP2) zur Verschlüsselung der personifizierten, sensiblen Daten verwendet wird,

dass die zwei Fingerprints (P-FP1/P-FP2) an einen zentralen Zugriffsserver (AAA) oder Trust Center übermittelt und dem Originators zugeordnet in einer Datenbank des Zugriffsservers abgespeichert werden,

dass zwei Fingerprints (M-FP1/M-FP2) eines Confidants an den zentralen Zugriffsserver (AAA) übermittelt und dem Confidant zugeordnet in der Datenbank des Zugriffsservers abgespeichert werden,

dass das Mobilfunkgeräts ein Daten-Verschlüsselungs- und -Transfermodul umfasst, wobei das Daten-Verschlüsselungs- und -Transfermodul mittels des Mobilfunkgerätes für den Originator zugreifbar ist und wobei entsprechende personifizierte, sensible Daten vom Originator mittels des Daten-Verschlüsselungs- und –Transfermodul aggregierbar und/oder validierbar und verschlüsselbar und über das Trust Center den Confidant über einen Datenübertragungskanal eines Datenübertragungsnetzwerkes transferrierbar sind,

dass die transferierten Daten vom Trust Center mittels einer Learning Machine und mittels des zweite Fingerprints (P-FP2) des Originators entschlüsselt werden, wobei mittels der Learning Machine personenrelevanten Daten der transferierten personifizierten, sensiblen Daten maskiert und/oder anonymisiert werden,

und wobei mittels der Learning Machine die maskierten und/oder anonymisierten Daten mittels des Fingerprints (M-FP1) des Confidant verschlüsselt mindestens teilweise an den Confidant und/oder Netzwerk-Nodes Dritter transferiert werden, und

dass die auf den Confidant oder die Netzwerk-Nodes Dritter transferierten, maskierten und/oder anonymisierten Daten durch den Confidant und/oder mittels der Netzwerk-Nodes der Dritten basierend auf dem Fingerprint (M-FP1) des Confidant entschlüsselt werden.

2. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach Anspruch 1, dadurch gekennzeichnet, dass der Originator ein medizinischer Patent ist, wobei die sensiblen, personifizierten Daten automatisiert von einer Learning Machine als Confidant und/oder Vertrauensarzt mittels einer Learning Machine Dritten zur weiteren Diagnostik und/oder Therapierung zur Verfügung gestellt werden.

3. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass das Mobilfunkgeräts des Originators mindestens einen Sensor zum Erfassen von biometrische Daten umfasst.

4. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach Anspruch 3, dadurch gekennzeichnet, dass mittels des mindestens einen Sensor zum Erfassen von biometrische Daten Finger-Prints erfassbar sind.

5. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der zentralen Zugriffsserver (AAA) einer Authentisierungs- und Autorisierungs-(AA)-Agency zugeordnet ist.

6. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der Confidant zur Entschlüsselung der personifizierten, sensiblen Daten mittels der Learning Machine auf die entsprechenden Fingerprints (P-FP1/P-FP2) des Originators auf dem zentralen Zugriffsserver (AAA) zugreift und auf die Learning Machine überträgt.

7. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Netzwerk-Nodes Dritter

zur Entschlüsselung der maskierten und/oder anonymisierten Daten auf die entsprechenden Fingerprints (M-FP1/M-FP2) des Confidant auf dem zentralen Zugriffsserver (AAA) zugreifen und auf sich übertragen.

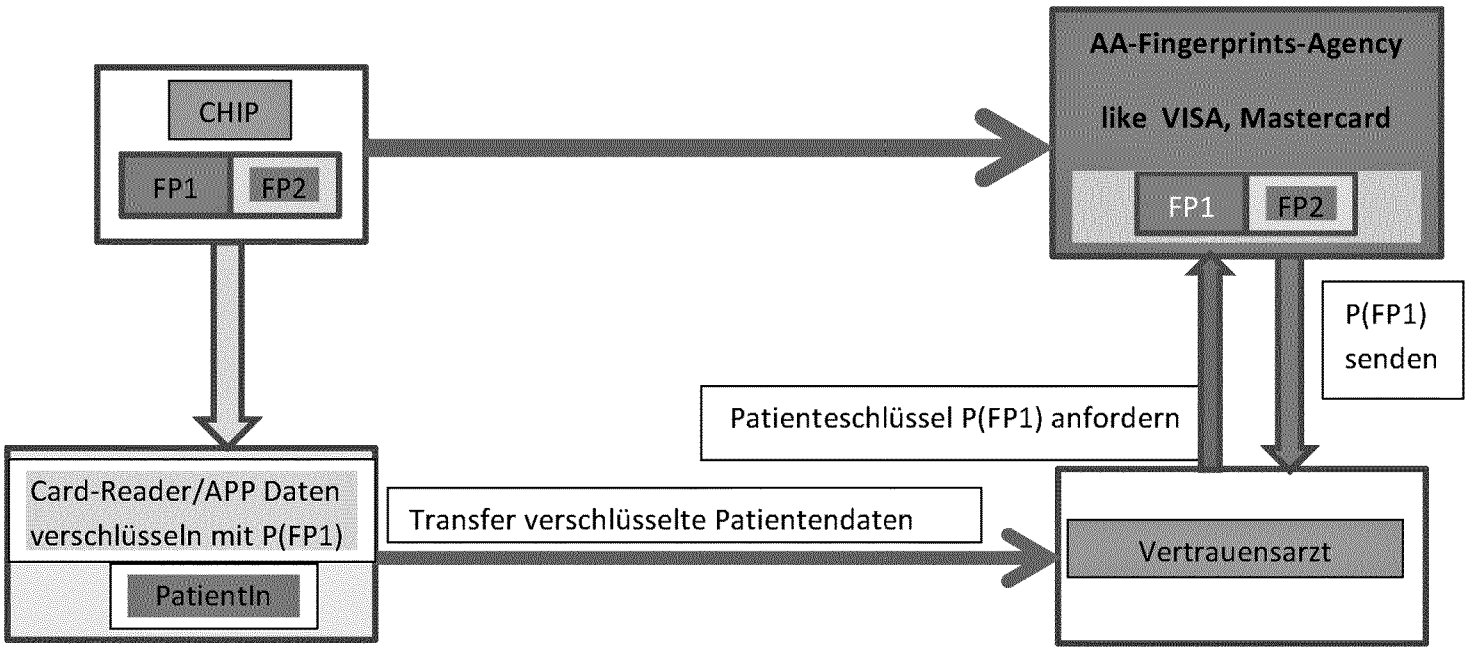
8. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass mittels der Learning Machine die entschlüsselten sensiblen, personifizierten Daten auf Daten-Konsistenz und Daten-Qualität überprüfbar sind.

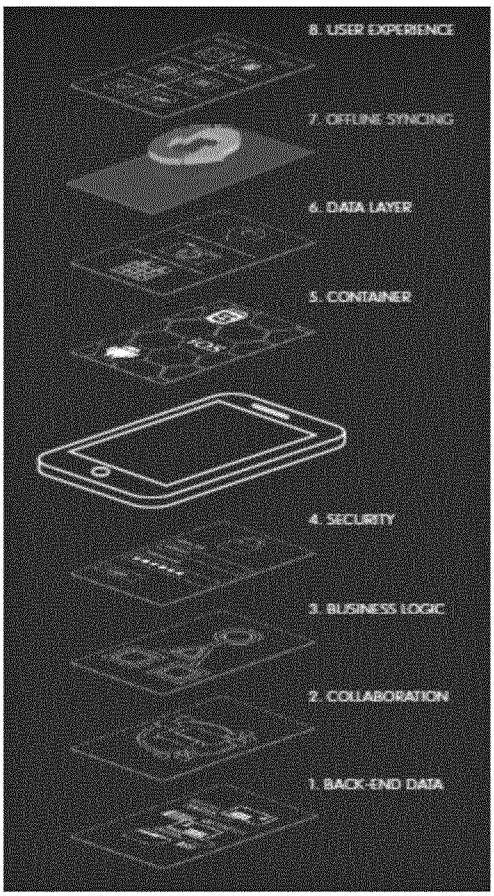
9. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass mittels der Learning Machine automatisiert oder durch den Confidant zwei oder mehr Aktivierungsstufen detektiert und dem Originator zugeordnet werden, wobei basierend auf den Aktivierungsstufen die Daten den Netzwerk-Nodes Dritter zugänglich gemacht werden.

10. Biometrischer, fingerprint-basierter Encryption-Decryption Engine nach Anspruch 9, dadurch gekennzeichnet, dass die Aktivierungsstufen mindestens die Triggerelemente "kein Handlungsbedarf" und/oder "Warnung" und/oder "Alarmzustand" umfassen.

FPC 1268 oder neuere Generation
+
iPhone
=
Personifierter iPhone für Patientendaten Transfer
Erweitern des FPC-Algorithmus
http://www.fingerprints.com/technology/algorithm/
1. für die Registrierung der zwei verschiedenen Finger, je eines aus jede Hand
2. speichern der Patientenfingerprints P(FP1) und P(FP2) lokal im iPhone
3. Verschlüsselungsalgorithmus mit P(FP2)
4. Menu-Führung akustisch (mehrere Sprachen) und visuel implementieren
5. Transfer der verschlüsselten Patientendaten
Zu 1:
Fingerprints registrieren
ein Finger aus jeder Hand
ein Finger für Authorisierung
ein Finger für Authentizierung
Daten für jeden Fingerprint in die lokale iPhone-Datenbank speichern
Zu 3: Verschlüsselungsalgorithmus E:
E(Daten-Klartext; P(FP2) = => verschlüsselte Daten

Fig. 1





Die APP Implementierung folgt den Regeln der State-of-the-Art, wie in

http://www.salesforce.com/platform/solutions/mobile/

aufgeführt.

Fig. 2

Prozessschritt 4:

1. Learning Machine maskiert alle Patient relevanten Daten (Namen, Vornamen, Geburtsdatum, Geschlecht, ...); Daten nur mit P(FP1), Authorisierungschlüssel versehen
2. Anonymisierte Patientendaten mit Schlüssel des Vertrauesarztes M(FP2) verschlüsseln E(Pat-Daten; M(FP2))
3. Senden der verschlüsselten Daten E(Pat-Daten; M(FP2)) an Forschungs-, Entwicklungszentrum, z.B. Nexus

Fig. 3

Schritt „2“
AA-Agency übermittelt an (F&E) den Schlüssel M(FP1)
AA-Fingerprints-Agency
Like VISA, Mastercard, ...
2
1
F&E
REI²AV
In F&E werden die verschlüsselten Patienten-Daten
E(Pat-Daten; M(FP2)) mit dem M(FP1) entschlüsselt
D(E(Pat-Daten; M(FP2)) = (Pat-Daten; M(FP2))
In den Patienten-Daten ist auch den
P(FP1), Authorisierungschlüssel des Patienten enthalten.
Mit der „Bio-Molecular Retrieval-Engine Intelligent Interactive Application Visualization“ (REI²AV) leistet die learning machine einen Beitrag, um den Match „Krankheits-Muster“ eines Patienten mit möglichen Medikamente, Therapien ... zu finden.

Fig. 4

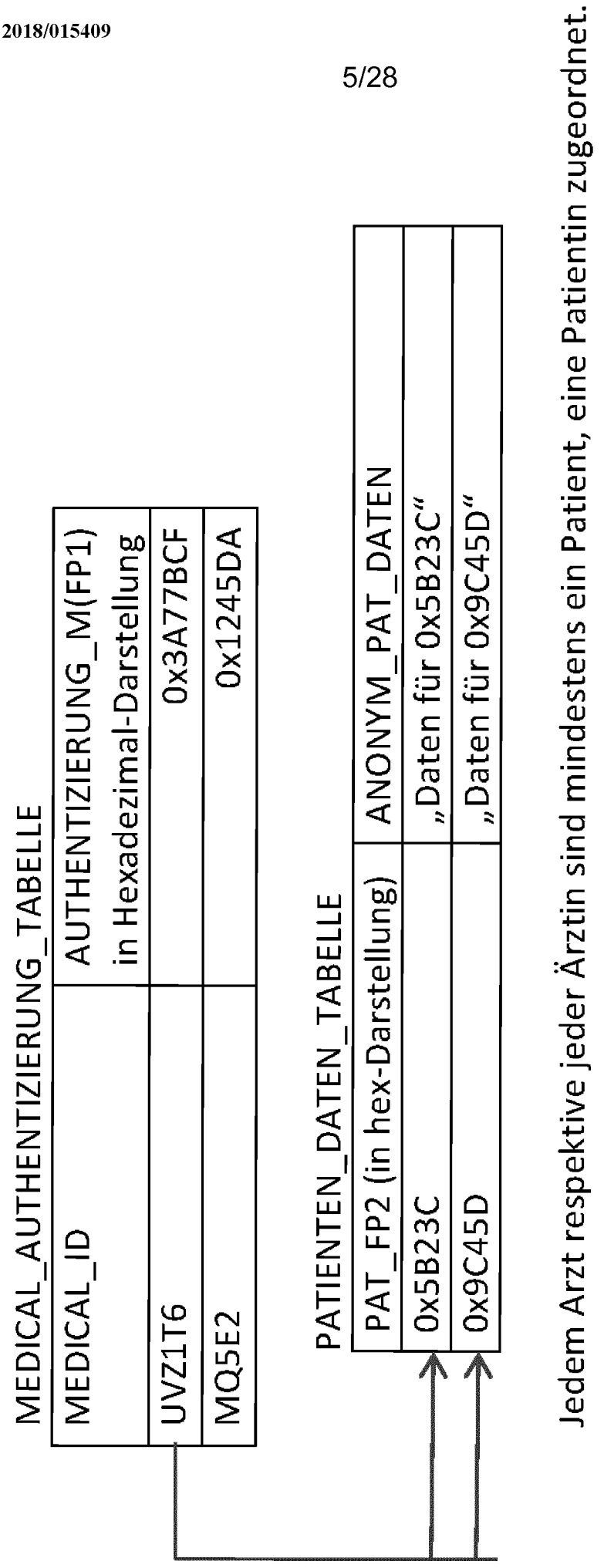

MEDICAL_AUTHENTIZIERUNG_TABELLE
MEDICAL_ID
AUTHENTIZIERUNG_M(FP1) in Hexadezimal-Darstellung
UVZ1T6
0x3A77BCF
MQ5E2
0x1245DA
PATIENTEN_DATEN_TABELLE
PAT_FP2 (in hex-Darstellung)
ANONYM_PAT_DATEN
0x5B23C
„Daten für 0x5B23C“
0x9C45D
„Daten für 0x9C45D“
Jedem Arzt respektive jeder Ärztin sind mindestens ein Patient, eine Patientin zugeordnet.

Fig. 5

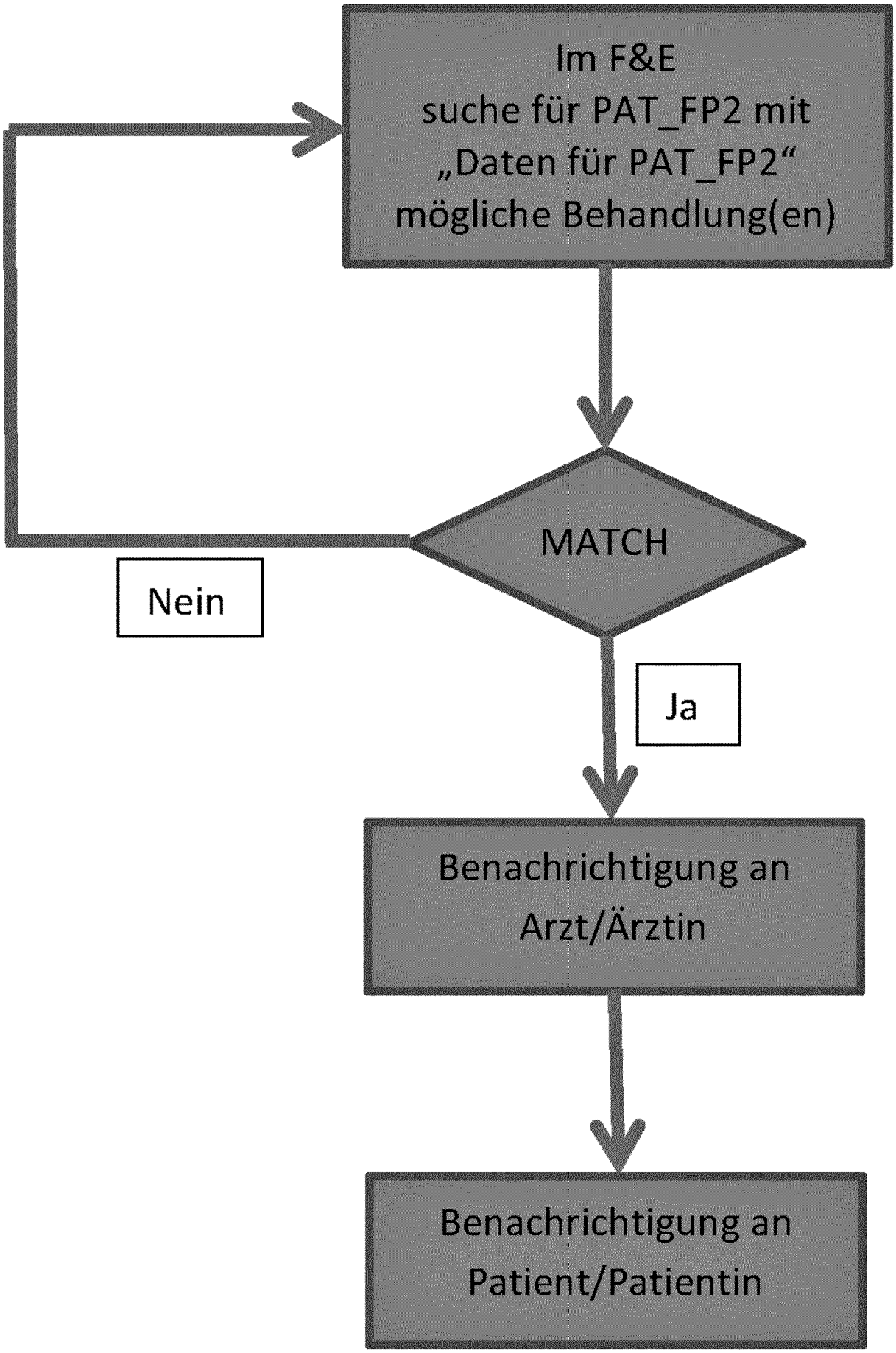

Im F&E
suche für PAT_FP2 mit
„Daten für PAT_FP2“
mögliche Behandlung(en)
MATCH
Nein
Ja
Benachrichtigung an
Arzt/Ärztin
Benachrichtigung an
Patient/Patientin

Fig. 6

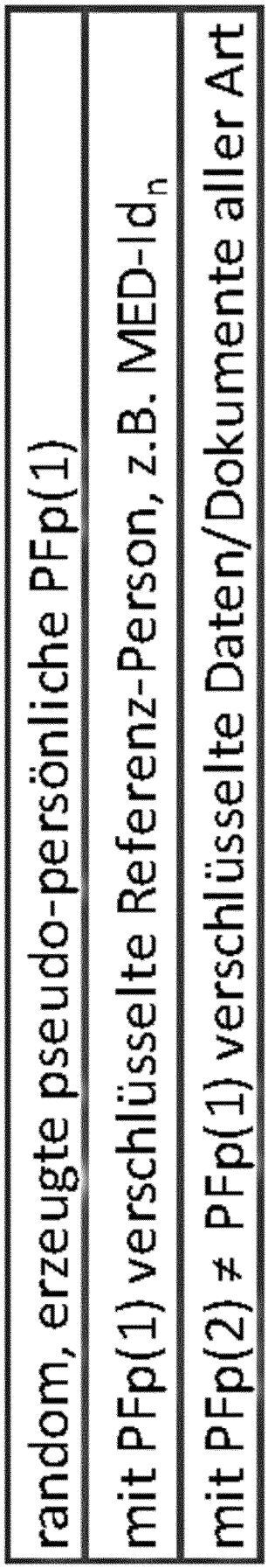

random, erzeugte pseudo-persönliche PFp(1)
mit PFp(1) verschlüsselte Referenz-Person, z.B. MED-Id$_n$
mit PFp(2) ≠ PFp(1) verschlüsselte Daten/Dokumente aller Art

Fig. 7

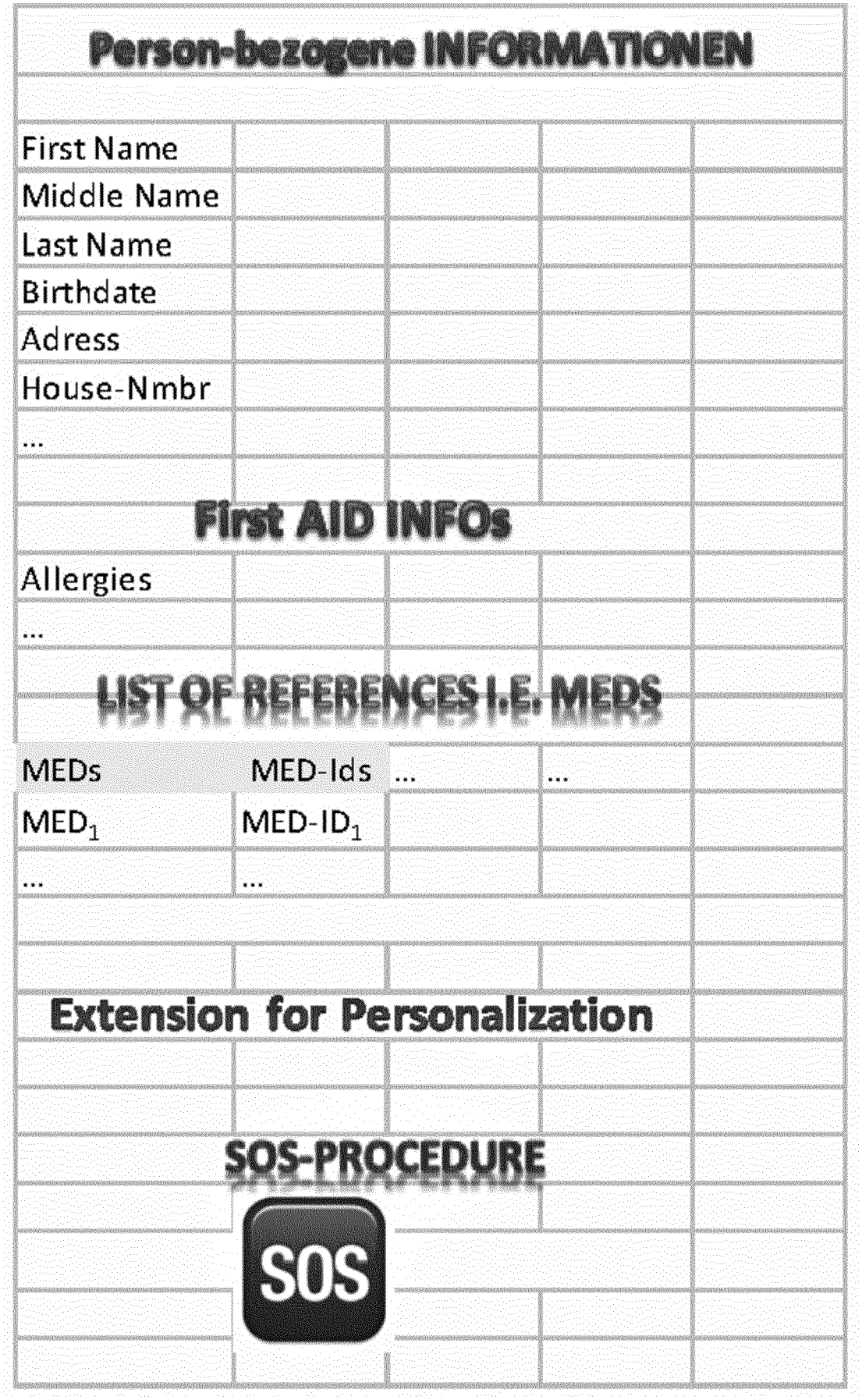

Person-bezogene INFORMATIONEN
First Name
Middle Name
Last Name
Birthdate
Adress
House-Nmbr
...
First AID INFOs
Allergies
...
LIST OF REFERENCES I.E. MEDS
MEDs
MED-Ids
...
...
MED1
MED-ID1
...
...
Extension for Personalization
SOS-PROCEDURE
SOS

Fig. 8a

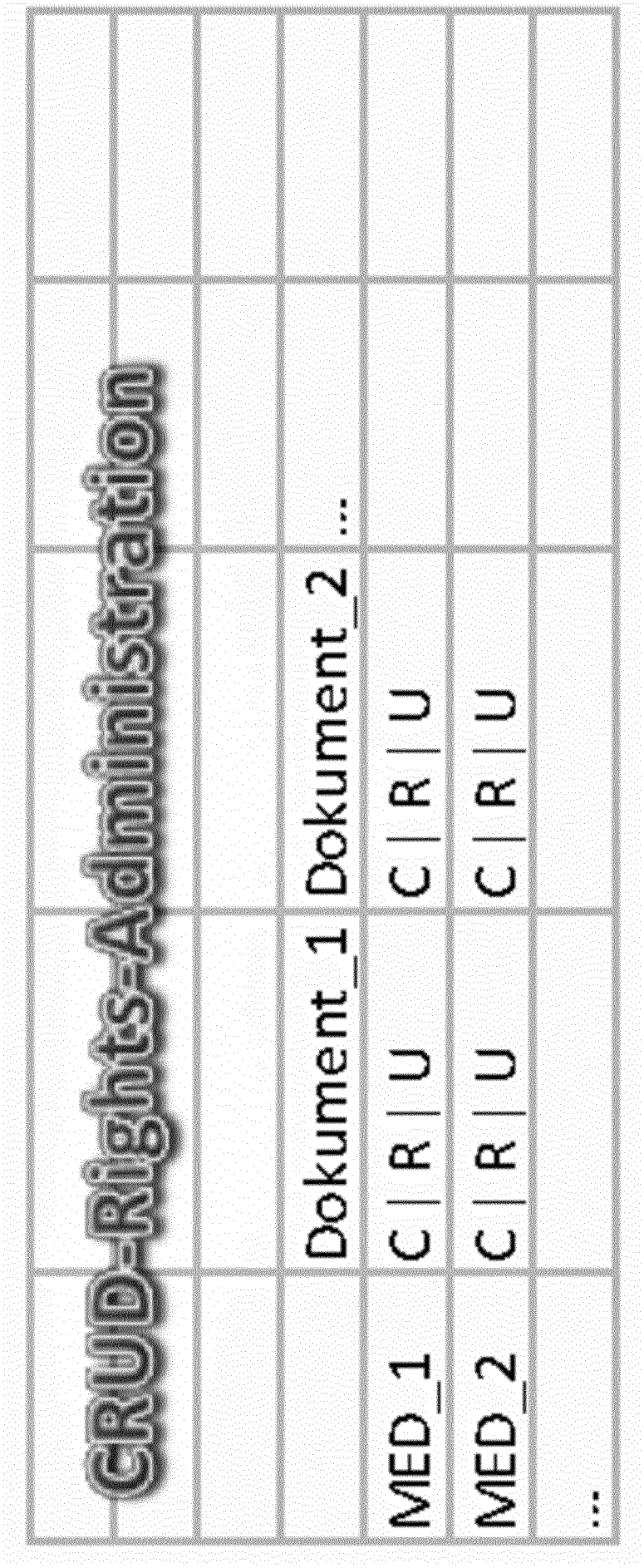

CRUD-Rights-Administration
Dokument_1
Dokument_2
...
MED_1
C | R | U
C | R | U
MED_2
C | R | U
C | R | U
...

Fig. 8b

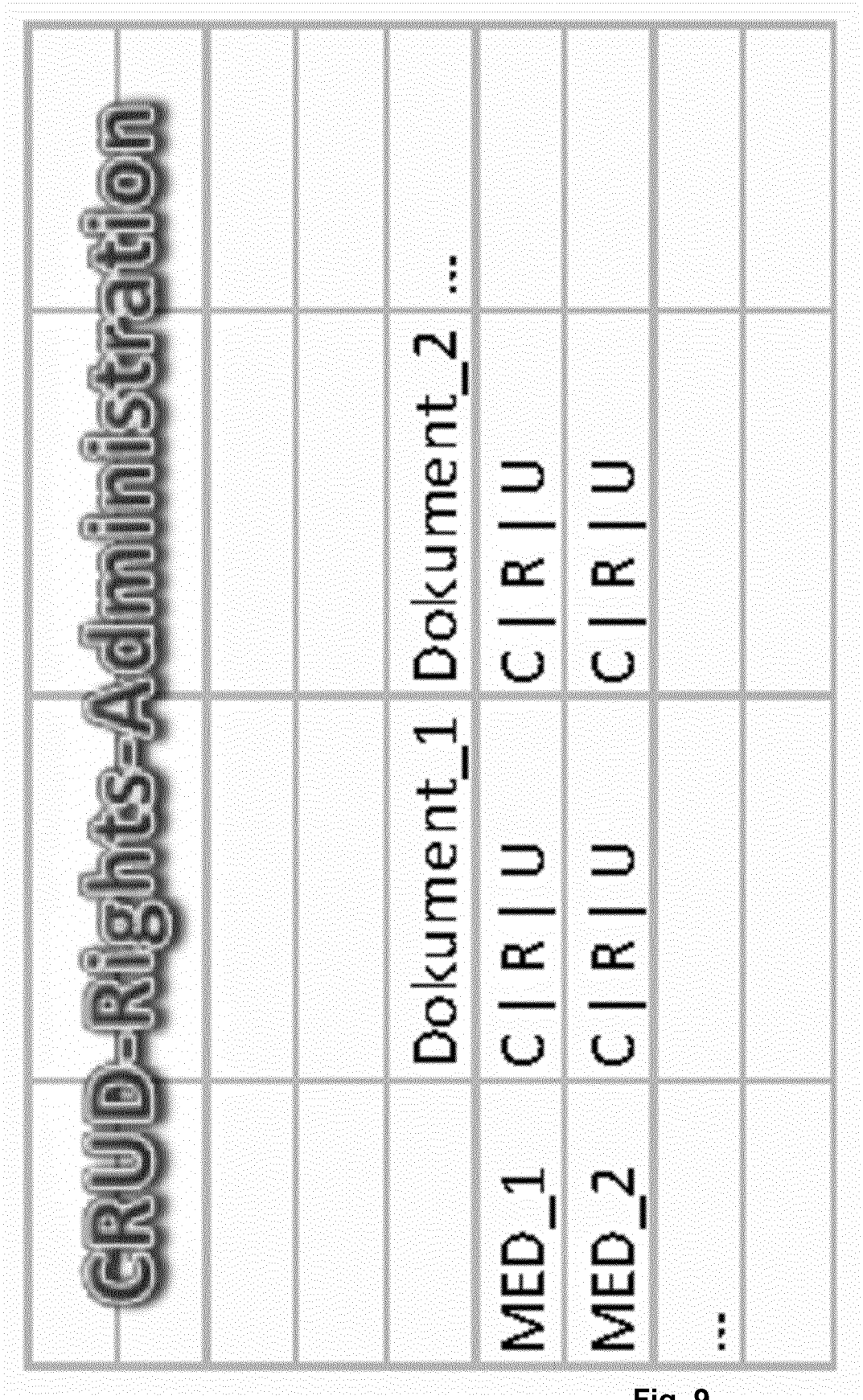

CRUD-Rights-Administration
Dokument_1
Dokument_2 ...
MED_1
C | R | U
C | R | U
MED_2
C | R | U
C | R | U
...

Fig. 9

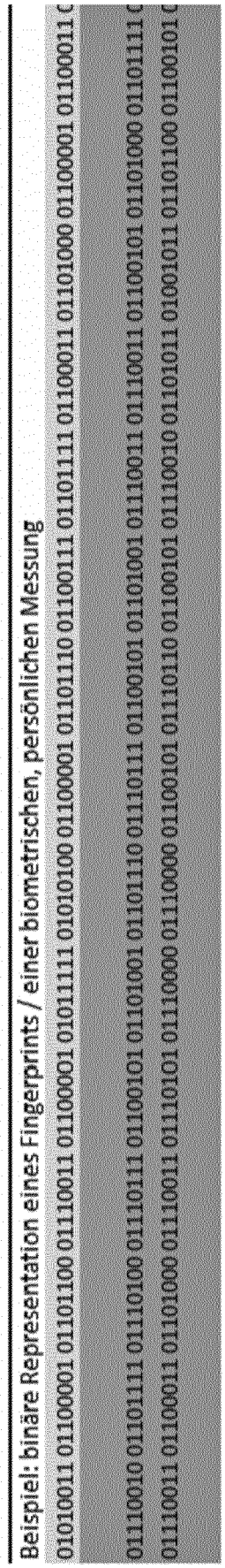

Beispiel: binäre Representation eines Fingerprints / einer biometrischen, persönlichen Messung
01010011 01100001 01101100 01110011 01100001 01011111 01010100 01100001 01101110 01100111 01101111 01100011 01101000 01100001 01100011
01110010 01101111 01101100 01110111 01001101 01101110 01101111 01100101 01101110 01100111 01101101 01101000 01101111
01110011 01100011 01101000 01100111 01101101 01100000 01100101 01100110 01101011 01101100 01001101

Fig. 10

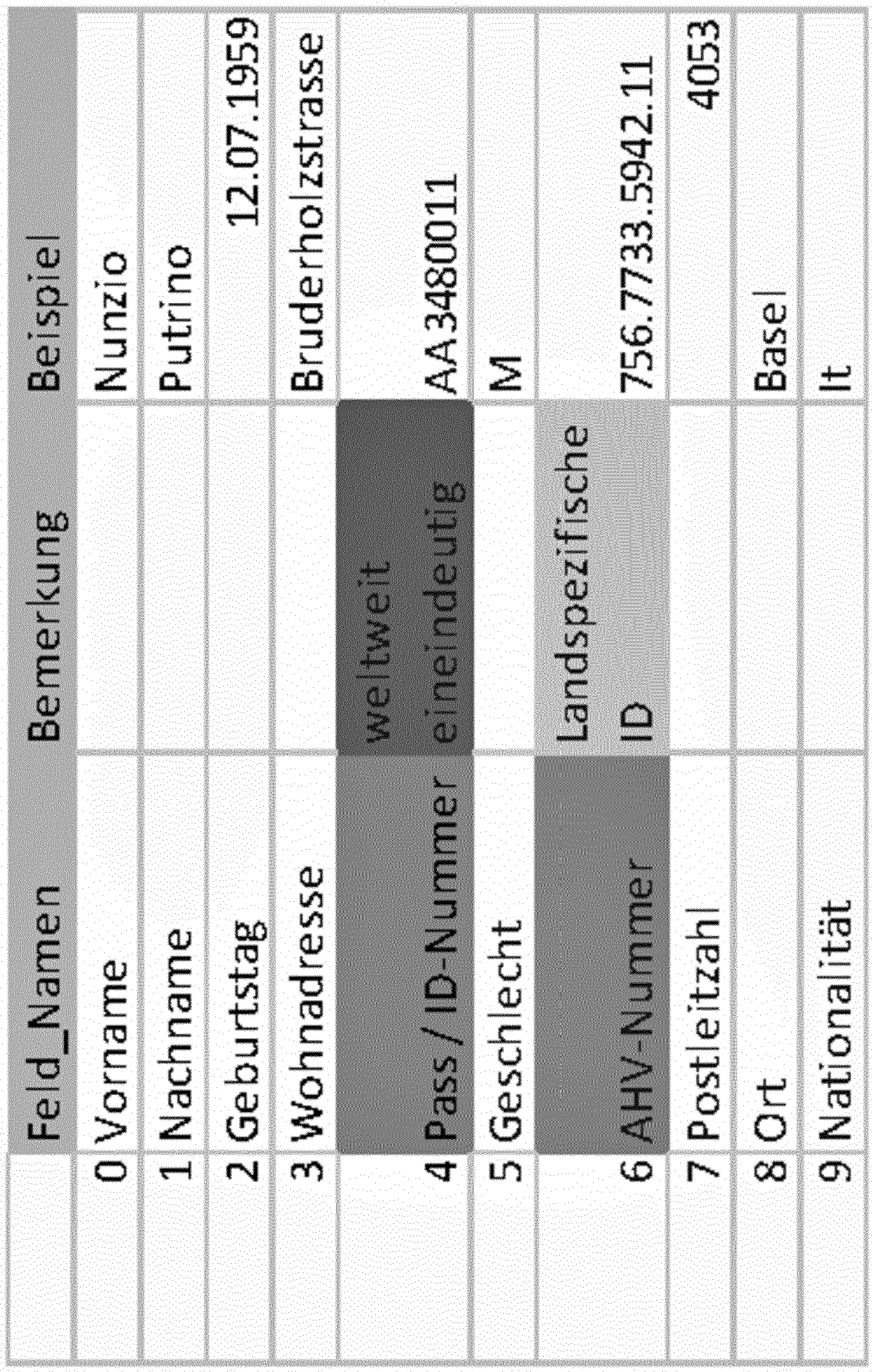
```
repeat(BOOL success, NSError *error) {
                if (success) {
                    NSLog(@"Auth was OK");
```

- **- -> getBitSequenceFingerPrintOne**
- **- -> generatePseudoPersonalizedKeyOne**
- **- -> startDialogForFingerPrintTwo**
- **- -> generatePseudoPersonalizedKeyTwo**

```
    }
    else {
     NSLog(@"Error received: %d", error);
```

- - -> **blockIntruder** }

Fig. 11



	Feld_Namen	Bemerkung	Beispiel
0	Vorname		Nunzio
1	Nachname		Putrino
2	Geburtstag		12.07.1959
3	Wohnadresse		Bruderholzstrasse
4	Pass / ID-Nummer	weltweit eineindeutig	AA3480011
5	Geschlecht		M
6	AHV-Nummer	Landspezifische ID	756.7733.5942.11
7	Postleitzahl		4053
8	Ort		Basel
9	Nationalität		It

Fig. 12

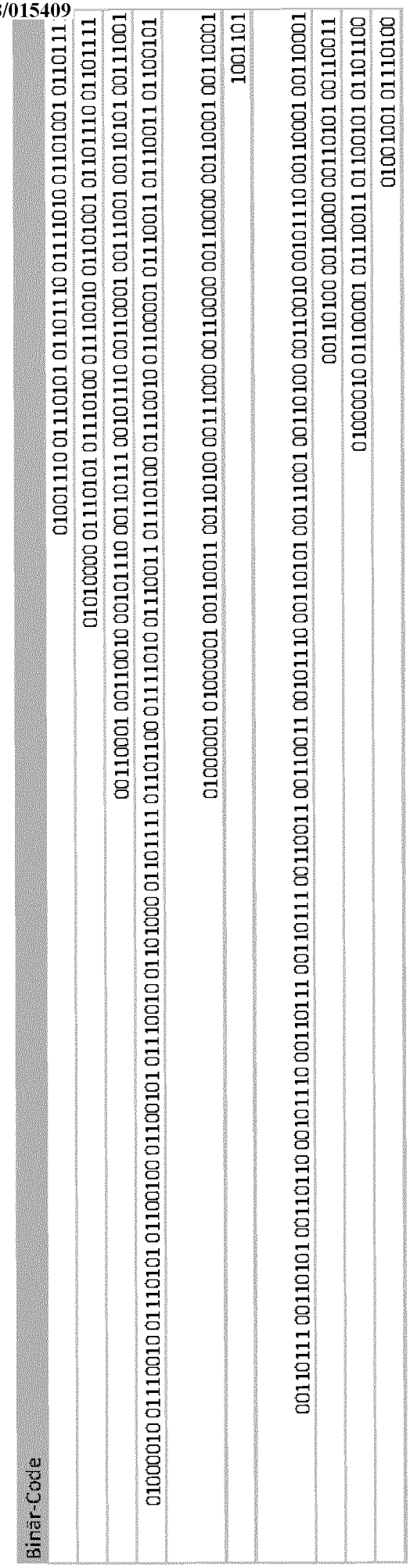

Binär-Code
01001110 01110101 01101110 01111010 01101001 01101111
01010000 01110101 01110100 01101010 01101001 01101110 01101111
00110001 00110010 00101110 00110111 00101110 00110001 00111001 00110001
01000010 01110010 01110101 01100100 01100101 01110011 01111010 01101100 01101111 01101000 01101111 01100010 01100101
01000001 01000001 00110011 00110100 00111000 00110000 00110000 00110001 00110001
1001101
00110111 00110101 00110110 00101110 00101110 00110111 00110011 00110011 00101110 00110100 00110101 00110101 00110001
00110000 00110000 00110101 00110011
01000010 01100001 01110011 01100101 01101100
01001001 01101000

Fig. 13

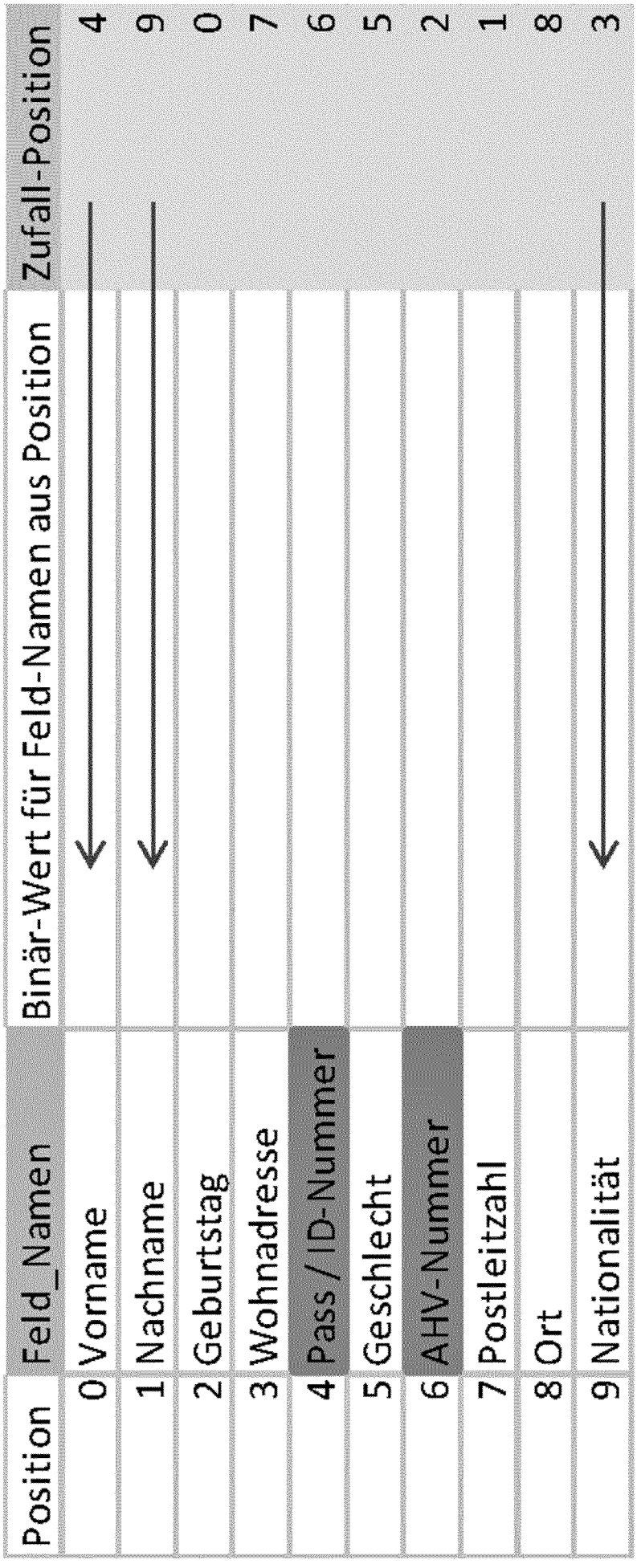

Position
Feld_Namen
Binär-Wert für Feld-Namen aus Position
Zufall-Position
0 Vorname
1 Nachname
2 Geburtstag
3 Wohnadresse
4 Pass / ID-Nummer
5 Geschlecht
6 AHV-Nummer
7 Postleitzahl
8 Ort
9 Nationalität
4 9 0 7 6 5 2 1 8 3

Fig. 14

Einrichten (Konfiguration) der APP				
Algorithmus im Mobile / Tablet / Desktop / Finger-Scanner/biometrical-Scanner				
auffordern ein von zehn Finger zu registrieren/erste biometrische Messung				
auffordern ein von den restlichen NEUN Finger zu registrieren/ zweite von der ersten biometrische Messung unabhängig				
Kontrolle BM 1 ≠ BM2	NEIN			
JA				
auffordern eine beliebige Zahlensequenz zwischen 0-9 einzugeben	Z_1			
auffordern eine beliebige Zahlensequenz zwischen 0-9 einzugeben	Z_2			
erzeugen einer Zufallssequenz $RZ_1(Z_1)$	RZ_1			
erzeugen einer Zufallssequenz $RZ_2(Z_2)$	RZ_2			
erzeuge Autorisierungs-Schlüssel mit FP_1 und Bit-Sequenz aus Zufallssequenz RZ1(Z1)	RAS_1			
erzeuge Autorisierungs-Schlüssel mit FP_2 und Bit-Sequenz aus Zufallssequenz RZ2(Z2)	RAS_2			
eröffne persönlicher Account bei einer AA-Agency				

Fig. 15

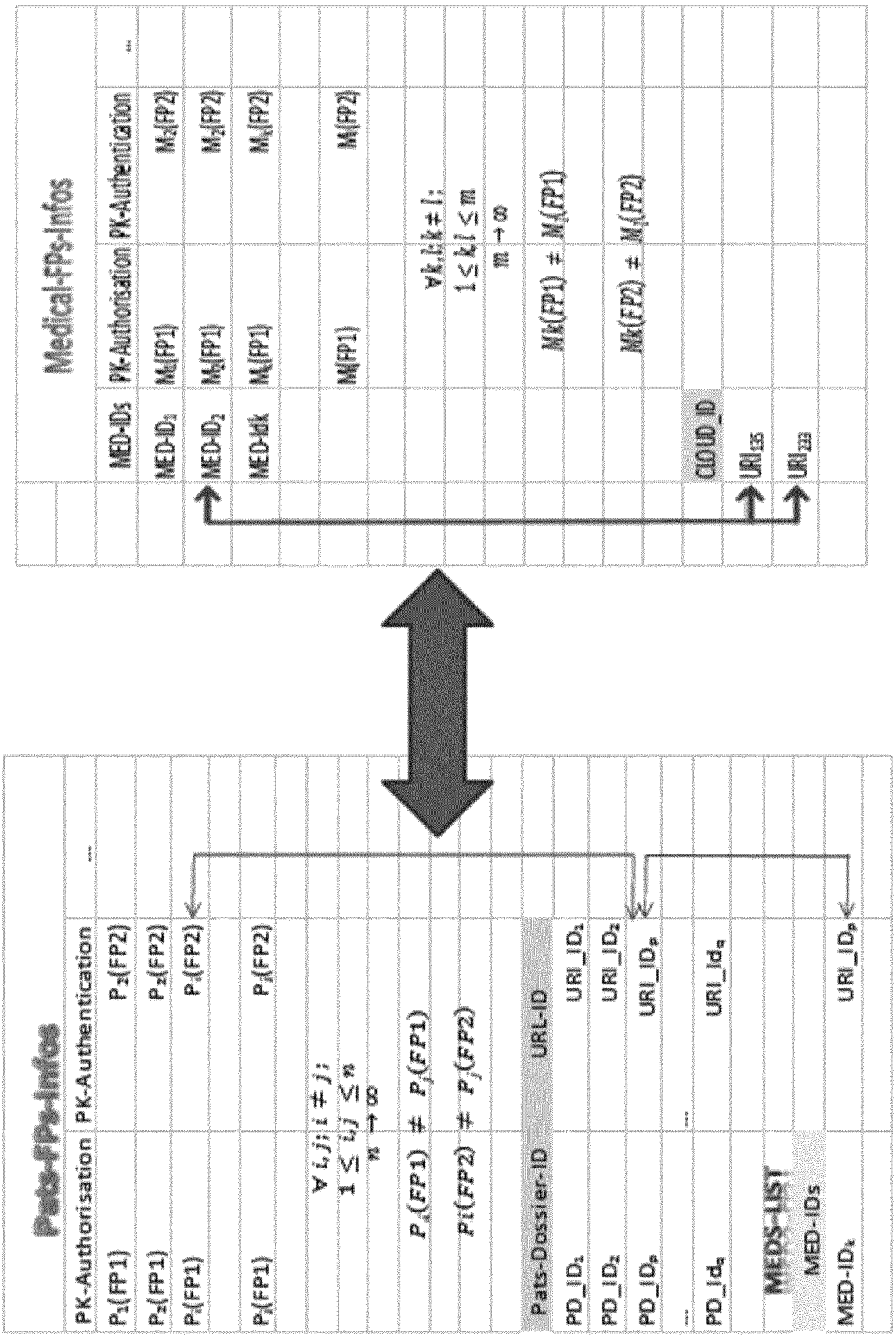

Medical-FPs-Infos
MED-ID3
PK-Authorisation
PK-Authentication
...
MED-ID1
M1(FP1)
M2(FP2)
MED-ID2
M2(FP1)
M3(FP2)
MED-Idk
Mk(FP1)
Mk(FP2)
M(FP1)
M(FP2)
∀k,l,k ≠ l;
1 ≤ k,l ≤ m
m → ∞
Mk(FP1) ≠ Mk(FP1)
Mk(FP2) ≠ Mk(FP2)
CLOUD_ID
URI125
URI233
Pats-FPs-Infos
PK-Authorisation
PK-Authentication
...
P1(FP1)
P2(FP2)
P2(FP1)
P3(FP2)
P1(FP1)
Pj(FP2)
∀ i,j; i ≠ j;
1 ≤ i,j ≤ n
n → ∞
Pi(FP1) ≠ Pj(FP1)
Pi(FP2) ≠ Pj(FP2)
Pats-Dossier-ID
URL-ID
PD_ID1
URI_ID1
PD_ID2
URI_ID2
PD_IDp
URI_IDp
...
PD_Idq
URI_Idq
MEDS-LIST
MED-IDs
MED-IDk
URI_IDp

Fig. 16

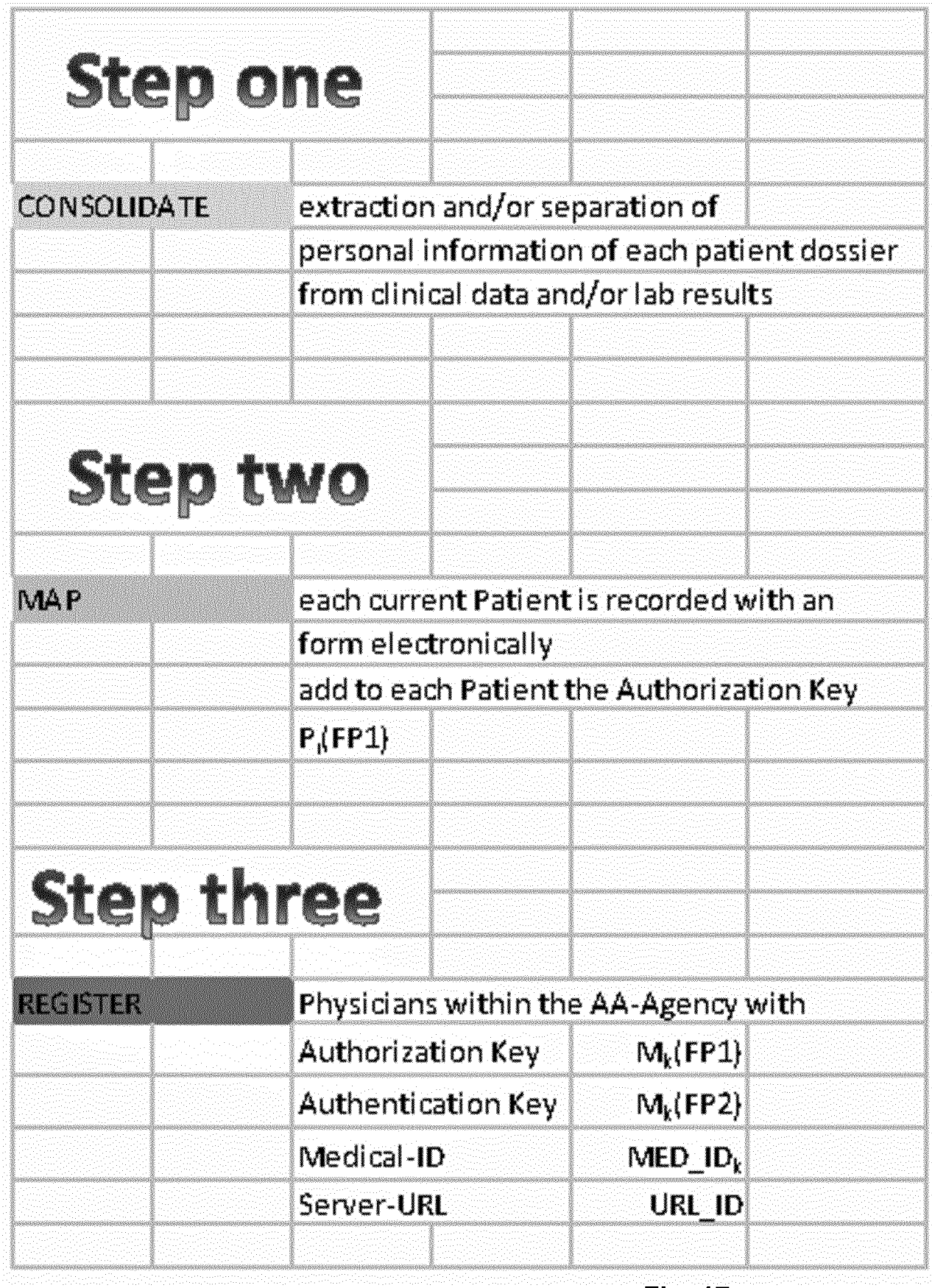

Step one
CONSOLIDATE
extraction and/or separation of
personal information of each patient dossier
from clinical data and/or lab results
Step two
MAP
each current Patient is recorded with an
form electronically
add to each Patient the Authorization Key
$P_i\{FP1\}$
Step three
REGISTER
Physicians within the AA-Agency with
Authorization Key
$M_k\{FP1\}$
Authentication Key
$M_k\{FP2\}$
Medical-ID
MED_ID_k
Server-URL
URL_ID

Fig. 17

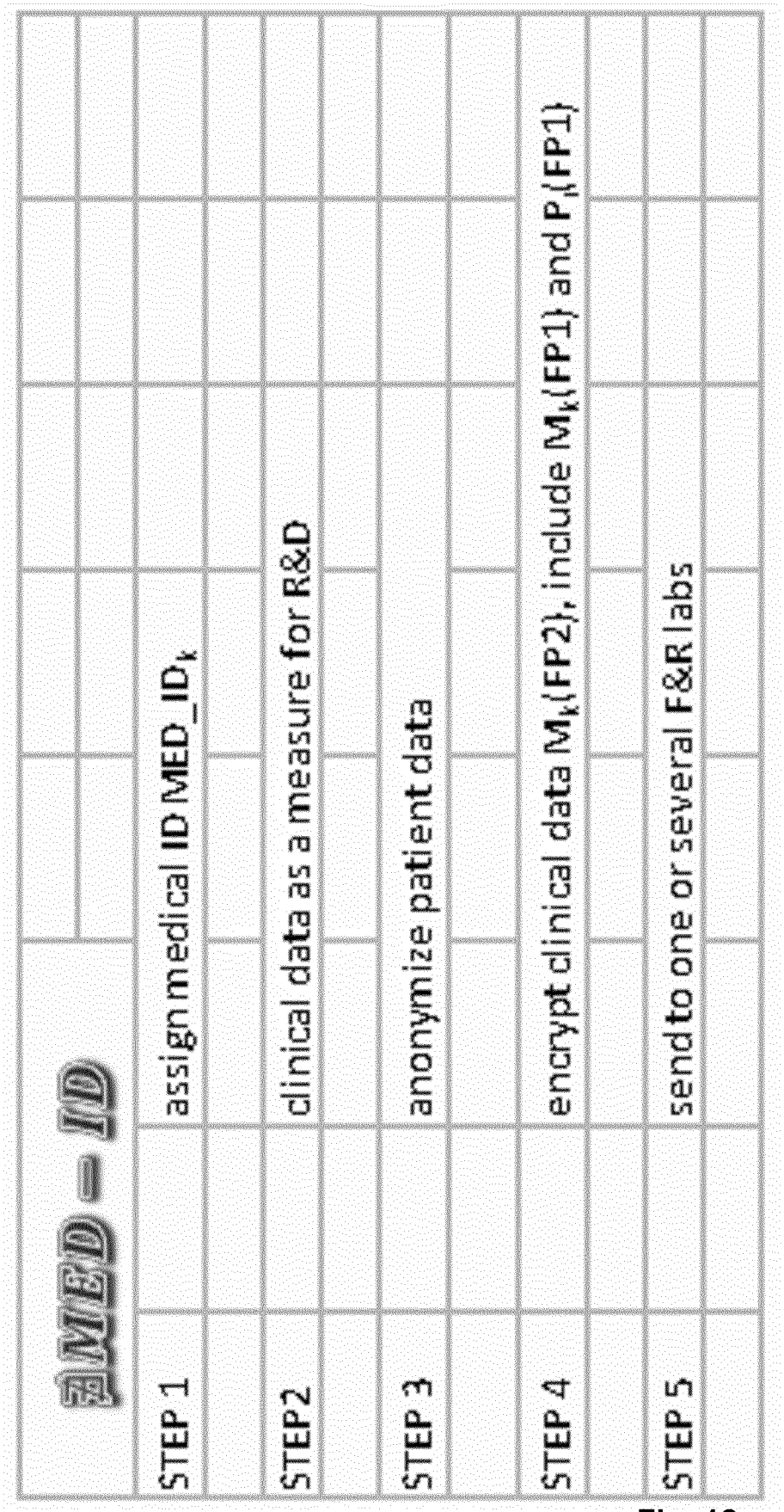

MED – ID
STEP 1
assign medical ID MED_ID$_k$
STEP2
clinical data as a measure for R&D
STEP 3
anonymize patient data
STEP 4
encrypt clinical data M_k(FP2), include M_k(FP1) and P_i(FP1)
STEP 5
send to one or several F&R labs

Fig. 18

∃! MED – ID	
STEP1	search for further MED_Ids
STEP 2	collect all URIs for MED_Ids
STEP 3	collect all Pat-Dossiers with Authorization Key P_i(FP1)
	at AA-Agency decrypt with P_k(FP2), encrypt with M_k(FP2)
STEP 4	local save complete Pat-Dossier and Decrypt with M_k(FP2)
STEP 5	organize Consilium in the virtual Chatroom
STEP 6	take only clinical data as a measure for R&D for an individual Patient
STEP 7	anonymize patient data
STEP 8	encrypt the clinical data with M_k(FP2), include M_k(FP1) and P_i(FP1)
STEP 9	send to one or several F&R labs

Fig. 19

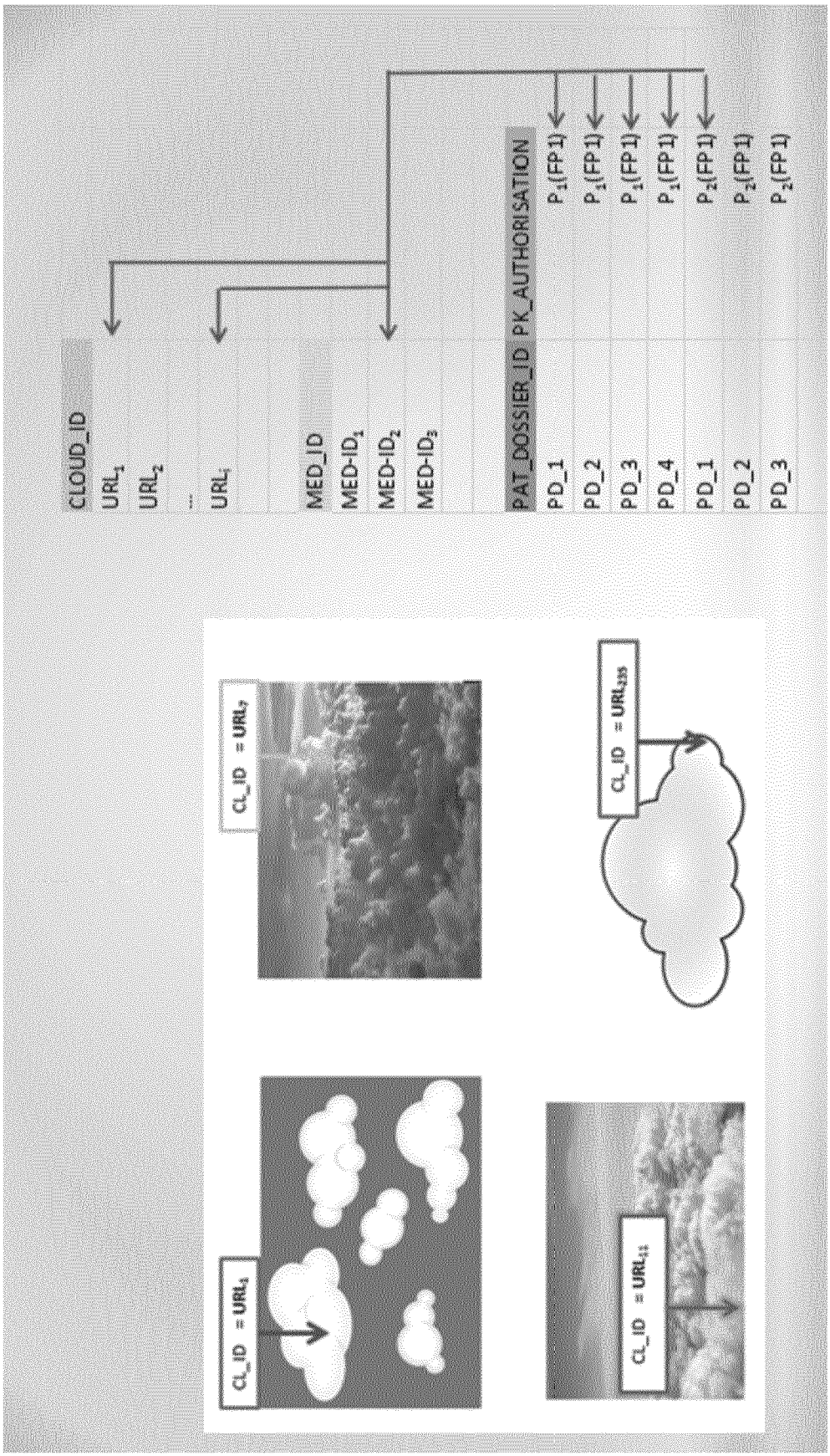

CLOUD_ID
URL1
URL2
...
URLi
MED_ID
MED-ID1
MED-ID2
MED-ID3
PAT_DOSSIER_ID PK_AUTHORISATION
PD_1 P1(FP1)
PD_2 P1(FP1)
PD_3 P1(FP1)
PD_4 P1(FP1)
PD_1 P2(FP1)
PD_2 P2(FP1)
PD_3 P2(FP1)
CL_ID = URL1
CL_ID = URL7
CL_ID = URL11
CL_ID = URL235

Fig. 20

Standard Form for R & D

MED-IDs	Medical-PK-Authorisation	Patient-PK-Authorisation	Question to R&D for individual Patient
MED-ID$_1$	$M_1\{FP1\}$	$P_j\{FP1\}$	$Q_{[1..n]}\{P_j\{FP1\}, M_1\{FP1\}\}$
MED-ID$_2$	$M_2\{FP1\}$	$P_i\{FP1\}$	$Q_{[1..n]}\{P_i\{FP1\}, M_2\{FP1\}\}$
MED-Id$_k$	$M_k\{FP1\}$	$P_q\{FP1\}$	$Q_{[1..n]}\{P_k\{FP1\}, M_q\{FP1\}\}$

Fig. 21

Decrypt anonymized Questions for individual Patient at the AA-Agency
DECRYPT with $M_i(FP2)$
D($Q_{[1..r]}(P_j(FP1), M_1(FP1)); M_1(FP2)$)
D($Q_{[1..f]}(P_i(FP1), M_2(FP1)); M_2(FP2)$)
D($Q_{[1..e]}(P_k(FP1), M_q(FP1)); M_q(FP2)$)
Encrypt anonymized Questions for individual Patient at the AA-Agency with R_D-Key
ENCRYPT with $R\_D\__i(FP2)$
E($Q_{[1..r]}(P_j(FP1), M_1(FP1)); R\_D_1\_(FP2)$))
E($Q_{[1..f]}(P_i(FP1), M_2(FP1)); R\_D_2\_(FP2)$))
E($Q_{[1..e]}(P_k(FP1), M_q(FP1)); R\_D_q\_(FP2)$))
Dencrypt anonymized Questions for individual Patient at the R&D-with R_D-Key
DECRYPT with R_D_i(FP2)
D($Q_{[1..r]}(P_j(FP1), M_1(FP1)); R\_D_1\_(FP2)$))
D($Q_{[1..f]}(P_i(FP1), M_2(FP1)); R\_D_2\_(FP2)$))
D($Q_{[1..e]}(P_k(FP1), M_q(FP1)); R\_D_q\_(FP2)$))

Fig. 22

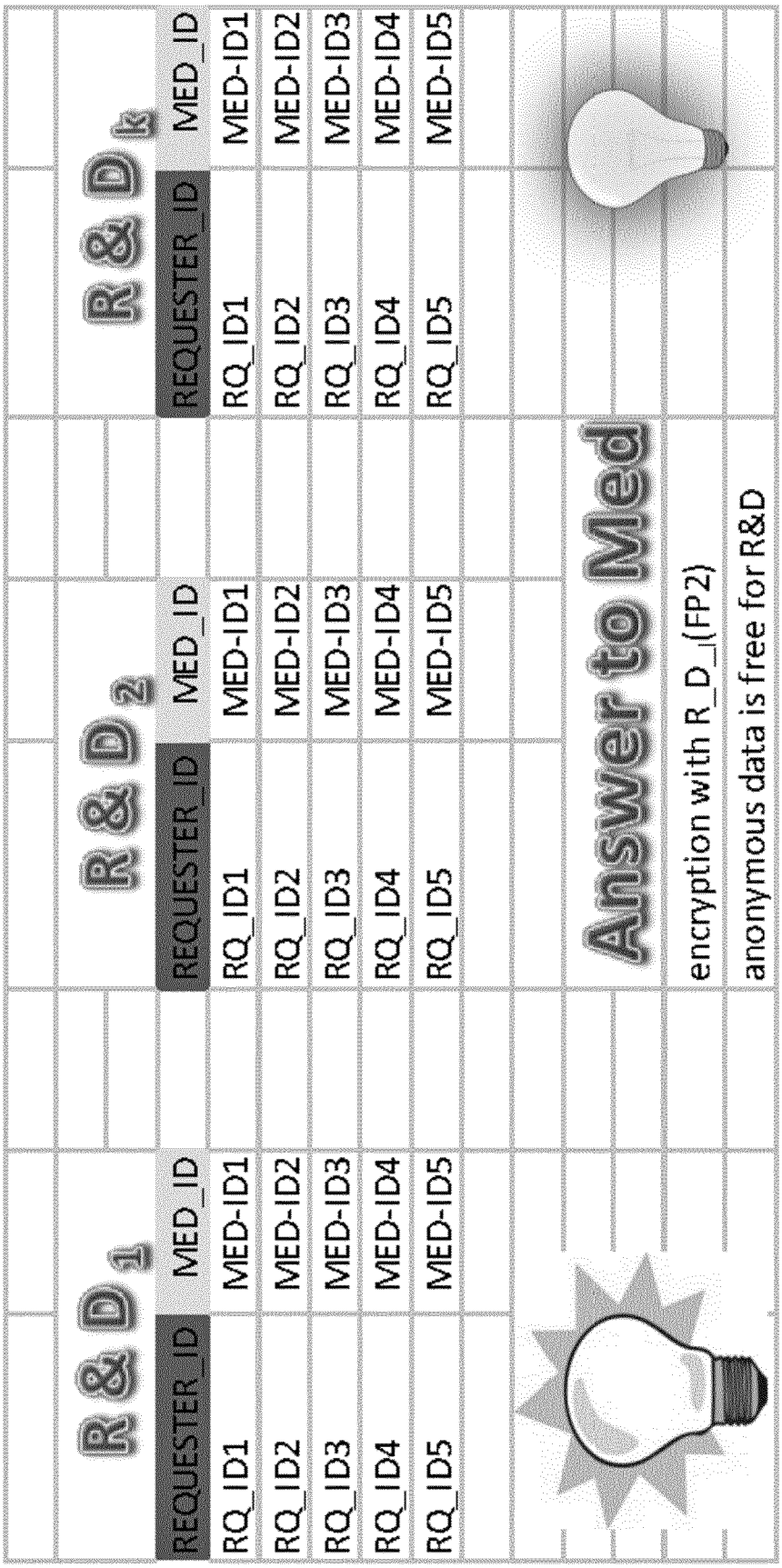

R & D 1
REQUESTER_ID
RQ_ID1
RQ_ID2
RQ_ID3
RQ_ID4
RQ_ID5
MED_ID
MED-ID1
MED-ID2
MED-ID3
MED-ID4
MED-ID5
R & D 2
REQUESTER_ID
RQ_ID1
RQ_ID2
RQ_ID3
RQ_ID4
RQ_ID5
MED_ID
MED-ID1
MED-ID2
MED-ID3
MED-ID4
MED-ID5
R & D k
REQUESTER_ID
RQ_ID1
RQ_ID2
RQ_ID3
RQ_ID4
RQ_ID5
MED_ID
MED-ID1
MED-ID2
MED-ID3
MED-ID4
MED-ID5
Answer to Med
encryption with R_D_i(FP2)
anonymous data is free for R&D

Fig. 23

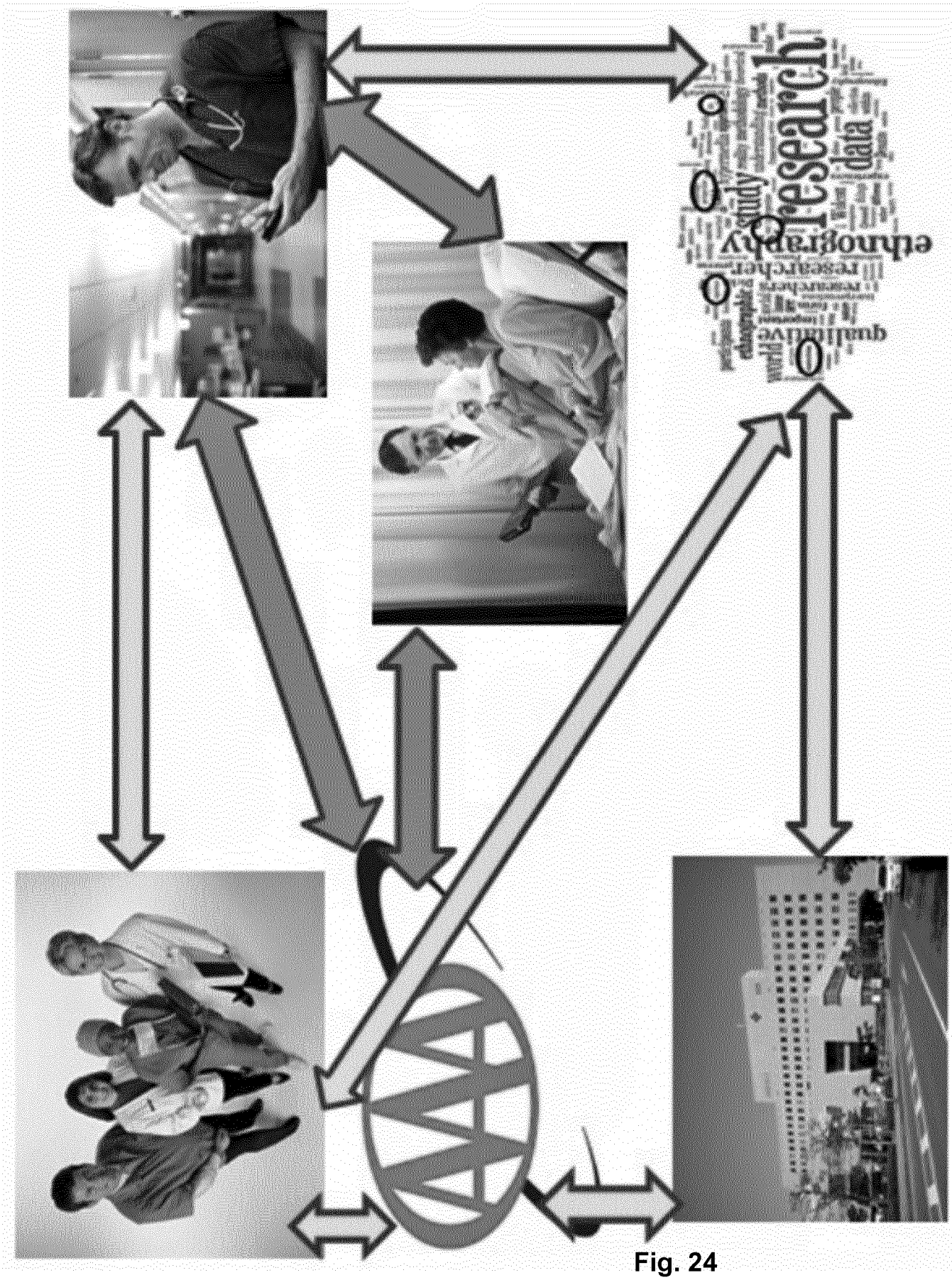


Fig. 24

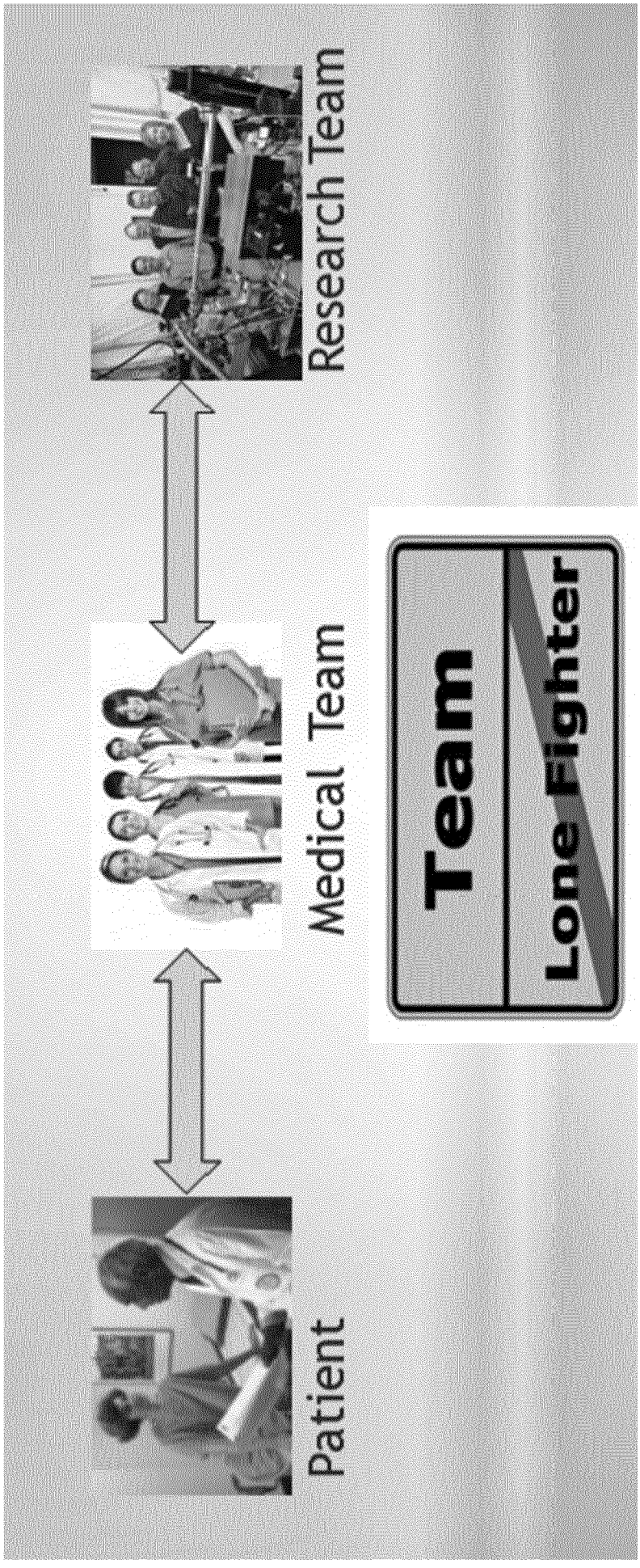


Fig. 25

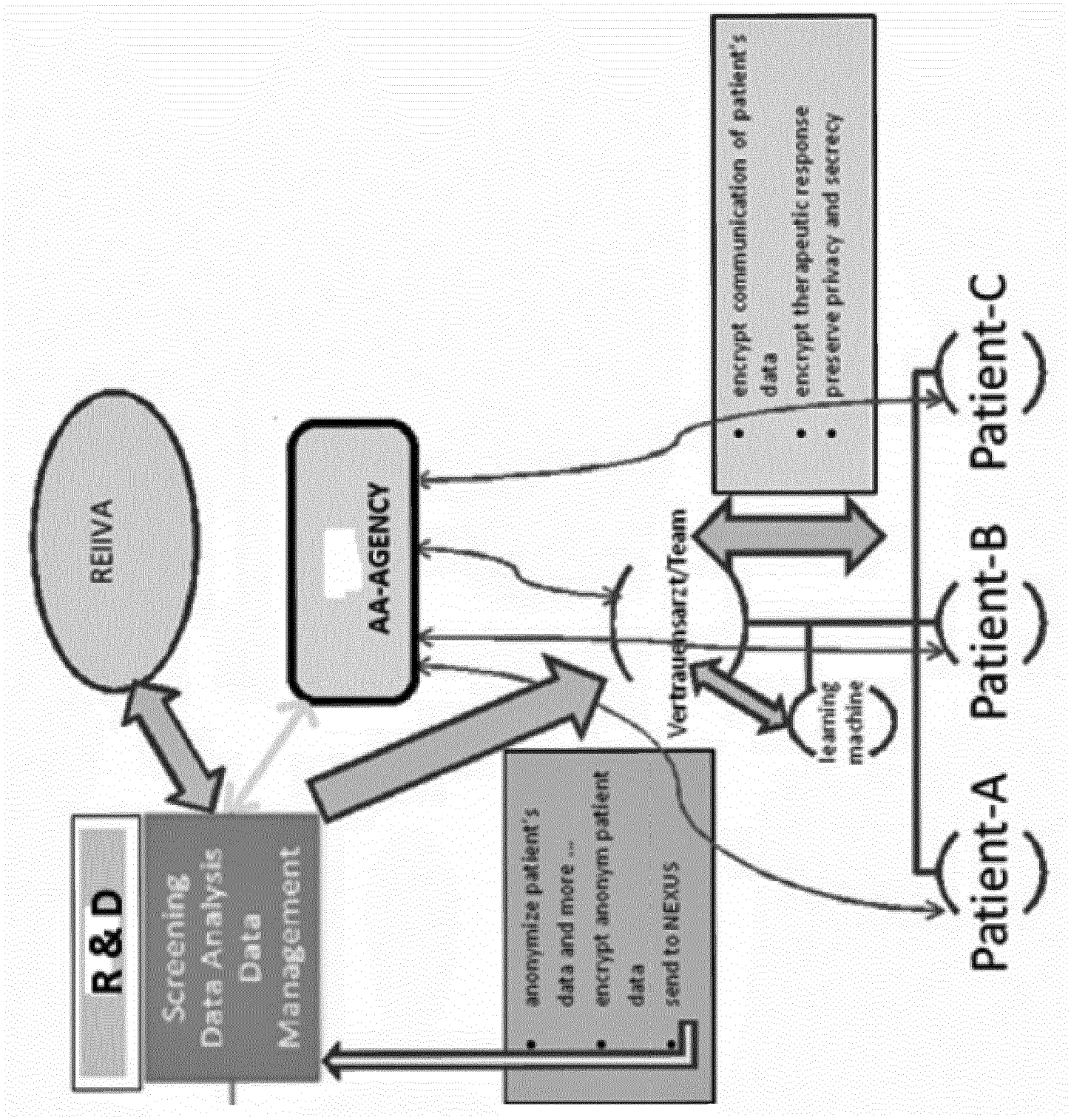

REIVA
AA-AGENCY
R & D
Screening
Data Analysis
Data
Management
anonymize patient's data and more ...
encrypt anonym patient data
send to NEXUS
Vertrauensarzt/Team
learning machine
encrypt communication of patient's data
encrypt therapeutic response
preserve privacy and secrecy
Patient-A
Patient-B
Patient-C

Fig. 26

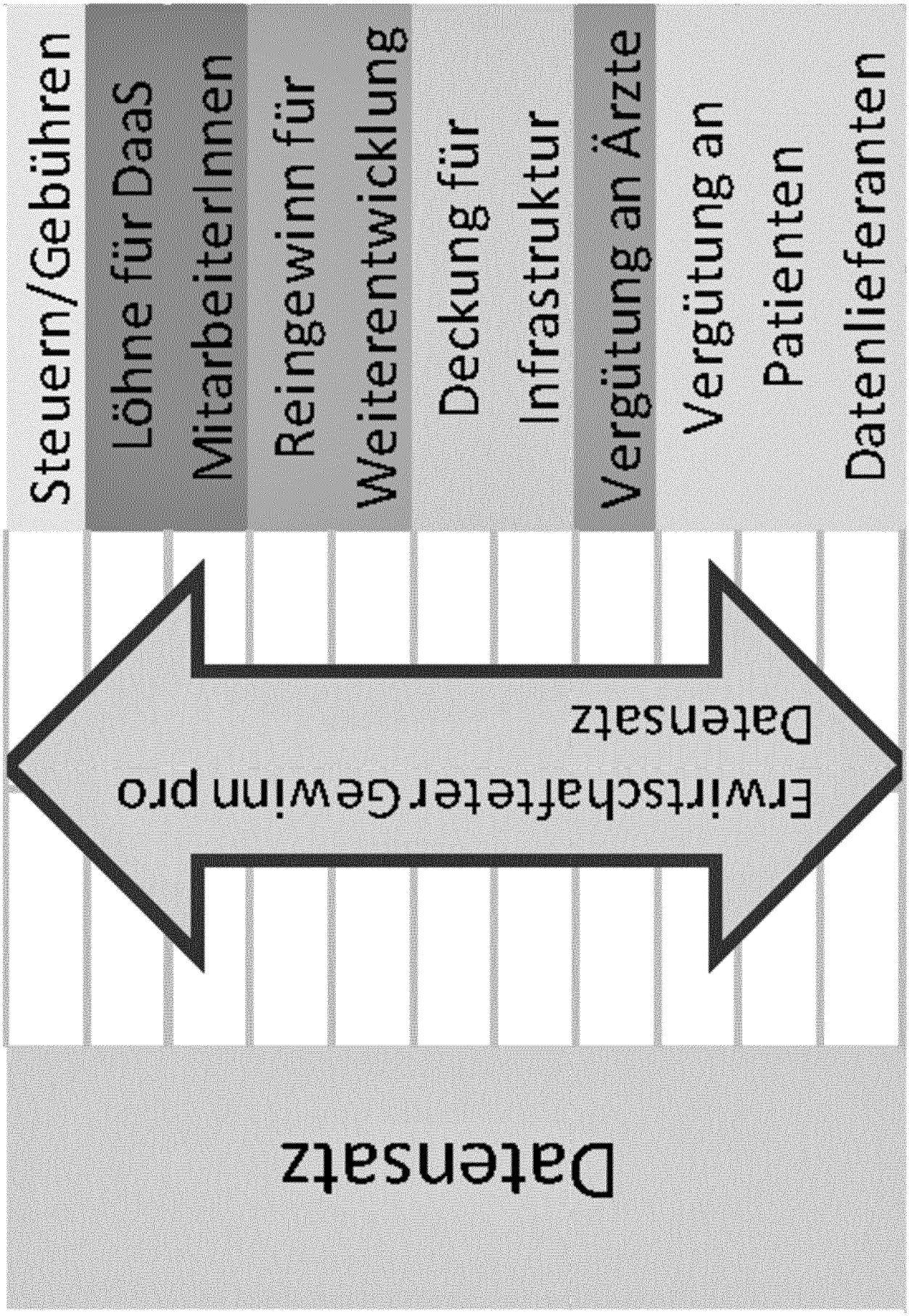

Steuern/Gebühren
Löhne für DaaS Mitarbeiterlnnen
Reingewinn für Weiterentwicklung
Deckung für Infrastruktur
Vergütung an Ärzte
Vergütung an Patienten
Datenlieferanten
Erwirtschafteter Gewinn pro Datensatz
Datensatz

Fig. 27

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/068169

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06F21/62 H04L9/00 H04L9/08 H04L9/32
ADD. H04L29/06

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)
G06F H04L

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/288874 A1 (HINKAMP THOMAS J [US]) 24 November 2011 (2011-11-24) paragraph [0035] paragraph [0041] paragraph [0049] paragraph [0050] figures 1,2A,5 paragraph [0036] paragraph [0063] paragraph [0060] paragraph [0059]	1-10

A	US 2011/078771 A1 (GRIFFIN STEPHANIE [US]) 31 March 2011 (2011-03-31) paragraph [0046] paragraph [0038] figure 3	1-10

	-/--	

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

[X] 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	Date of mailing of the international search report
14 September 2017	27/09/2017

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, Fax: (+31-70) 340-3016	De la Hera, Germán

2

Form PCT/ISA/210 (second sheet) (April 2005)

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 2002/010679 A1 (FELSHER DAVID PAUL [US]) 24 January 2002 (2002-01-24) paragraph [0220] paragraph [0293] - paragraph [0296] paragraph [0042] - paragraph [0043] figure 2 -----	1-10
A	US 2007/279187 A1 (HEKMATPOUR SHAHROOZ [US] ET AL) 6 December 2007 (2007-12-06) paragraph [0081] paragraph [0040] paragraph [0085] paragraph [0048] figure 3 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/068169

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011288874 A1	24-11-2011	NONE	
US 2011078771 A1	31-03-2011	US 2011078771 A1	31-03-2011
		WO 2011041616 A1	07-04-2011
US 2002010679 A1	24-01-2002	AU 7182701 A	21-01-2002
		US 2002010679 A1	24-01-2002
		US 2008306872 A1	11-12-2008
		US 2009287837 A1	19-11-2009
		WO 0205061 A2	17-01-2002
US 2007279187 A1	06-12-2007	US 2007279187 A1	06-12-2007
		WO 2007120793 A2	25-10-2007

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/068169

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/32 G06F21/62 H04L9/00 H04L9/08 H04L9/32
ADD. H04L29/06

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04L

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, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2011/288874 A1 (HINKAMP THOMAS J [US]) 24. November 2011 (2011-11-24) Absatz [0035] Absatz [0041] Absatz [0049] Absatz [0050] Abbildungen 1,2A,5 Absatz [0036] Absatz [0063] Absatz [0060] Absatz [0059] -----	1-10
A	US 2011/078771 A1 (GRIFFIN STEPHANIE [US]) 31. März 2011 (2011-03-31) Absatz [0046] Absatz [0038] Abbildung 3 -----	1-10

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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	Absendedatum des internationalen Recherchenberichts
14. September 2017	27/09/2017

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	De la Hera, Germán

2

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2002/010679 A1 (FELSHER DAVID PAUL [US]) 24. Januar 2002 (2002-01-24) Absatz [0220] Absatz [0293] - Absatz [0296] Absatz [0042] - Absatz [0043] Abbildung 2 -----	1-10
A	US 2007/279187 A1 (HEKMATPOUR SHAHROOZ [US] ET AL) 6. Dezember 2007 (2007-12-06) Absatz [0081] Absatz [0040] Absatz [0085] Absatz [0048] Abbildung 3 -----	1-10

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/068169

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2011288874 A1	24-11-2011	KEINE	
US 2011078771 A1	31-03-2011	US 2011078771 A1	31-03-2011
		WO 2011041616 A1	07-04-2011
US 2002010679 A1	24-01-2002	AU 7182701 A	21-01-2002
		US 2002010679 A1	24-01-2002
		US 2008306872 A1	11-12-2008
		US 2009287837 A1	19-11-2009
		WO 0205061 A2	17-01-2002
US 2007279187 A1	06-12-2007	US 2007279187 A1	06-12-2007
		WO 2007120793 A2	25-10-2007