

發明專利說明書

(填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫)

※ 申請案號： 911×3258 ※IPC 分類： G06F15/00
※ 申請日期： 91.10.9

壹、發明名稱

(中文) 用於病患資料之資料處理系統

(英文) Data processing system for patient data

貳、發明人 (共 6 人)

發明人 1 (如發明人超過一人，請填說明書發明人續頁)

姓名：(中文) 克利斯提昂.提爾雪

(英文) THIELSCHER, Christian

住居所地址：(中文) 德國 D-51469 貝基許 葛拉德巴哈,費爾德街 94 號

(英文) Feldstrasse 94, D-51469 Bergisch Gladbach, Germany

國籍：(中文) 德國

(英文) Germany

參、申請人 (共 1 人)

申請人 1 (如發明人超過一人，請填說明書申請人續頁)

姓名或名稱：(中文) 辛巴西斯股份有限公司

(英文) Symbasis GmbH

住居所或營業所地址：(中文) 德國 D-53859 尼德卡塞-蒙多夫,史佩莎特街 5a

(英文) Spessartstr 5a, D-53859 Niederkassel-Mondorf, Germany

國籍：(中文) 德國

(英文) Germany

代表人：(中文) 克利斯提昂.提爾雪

(英文) THIELSCHER, CHRISTIAN

☐ 續發明人或申請人續頁 (發明人或申請人欄位不敷使用時，請註記並使用續頁)

發明人 2

姓名：(中文) 馬汀.哥特費爾德

(英文) GOETTFRIED, Martin

住居所地址：(中文) 德國 D-61462 柯尼希斯坦,候依候爾路 6b

(英文) Heuhohlweg 6b, D-61462 Koenigstein, Germany

國籍：(中文) 德國

(英文) Germany

發明人 3

姓名：(中文) 西蒙.巫姆布萊特

(英文) UMBREIT, Simon

住居所地址：(中文) 德國 D-71720 歐伯史特費爾德,哥德街 19 號

(英文) Goethestrasse 19, D-71720 Oberstenfeld, Germany

國籍：(中文) 德國

(英文) Germany

發明人 4

姓名：(中文) 法蘭克.波格納

(英文) BOEGNER, Frank

住居所地址：(中文) 德國 D-71686 雷姆塞克,涅卡哈德 24 號

(英文) In der Neckarhalde 24, D-71686 Remseck, Germany

國籍：(中文) 德國

(英文) Germany

發明人 5

姓名：(中文) 尤亨.哈克

(英文) HAACK, Jochen

住居所地址：(中文) 德國 D-60325 法蘭克福,薩維尼街 37 號

(英文) Savignystrasse 37, D-60325 Frankfurt a. M. Germany

國籍：(中文) 德國

(英文) Germany

發明人 6

姓名：(中文) 尼克來.施洛德

(英文) SCHROEDERS, Nikolai v.

住居所地址：(中文) 德國 D-45549 史普洛克霍夫,中間街 8 號

(英文) Mittelstrasse 8 ,D-45549 Sprockhoevel ,Germany

國籍：(中文) 德國

(英文) Germany

捌、聲明事項

☐ 本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間，其日期為：_____

☐ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號 順序註記】

1. _____
2. _____
3. _____

☒ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號 順序註記】

1. 德國；2001.10.11；101 50 008.4
2. 德國；2001.02.27；102 09 780.1
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號 順序註記】

1. _____
2. _____
3. _____

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

1. _____
2. _____
3. _____

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

1. _____
2. _____
3. _____

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明

【發明所屬之技術領域】

本發明係關於用於一種病患資料的處理之資料處理系統，該病患資料係包含每一個病患之個人辨識資料及對應之健康資料。該病患資料的處理之資料處理系統係包含一或者多個中央位置。每一個中央位置係包含一個儲存健康資料之資料庫及連接至該資料庫之入口裝置。該病患之健康資料係能夠透過該入口裝置而由該資料庫取得及／或儲存於該資料庫之中。

【先前技術】

近來，於健康服務之嘗試係增加，以藉由健康資料之一個最佳化處理而有效地改進病患處理之成本，該資料係敘述健康狀態及每一個個別病患之處理。爲了此目的，一個互相連結之系統係有用的，透過該互相連結之系統，牽涉到一個病患之治療之不同健康專家，諸如，醫師，藥劑師及類似健康保險或者州立醫院之治療之付款者係能夠獲得對於需要更有效率之特定健康資料之接取。如此之系統係目前於關鍵字“電子健康記錄”，“健康照顧卡”，“健康卡”或者“健康照顧資料系統”之下被討論。

然而，一個病患之健康資料係爲高度敏感的，且因此，必須受限於相當嚴格之資料保護，以避免非牽涉到該治療之非被授權人員或者其他人員可能接取儲存之健康資料。

本發明所解決之技術問題係爲提供一個用於病患資料

之處理的獨特的資料保護系統，其中，該健康資料係儲存於具有非常高度保護而防止非被授權之接取之中央資料庫內。

本發明係藉由提供一個具有申請專利範圍第 1 項之特性之資料處理系統而解決此問題。於該系統中，該健康資料係不指定至該個別中央資料庫中之個別病患資料而儲存，使未獲授權之人員無法指定該資料至特定之個人，即使其能夠由該資料庫取出健康資料。

對於一個個別病患之健康資料之獲授權接取及取出係需要指定至該病患之一個個別資料記錄辨識元碼之輸入端。透過該碼，一個對應之健康資料記錄（或者該記錄之一個特定部分）係能夠由一個中央資料庫取得。然而，該碼係可由該個人辨識資料分離。此意謂該被取得之健康資料係不能夠單獨藉由該碼而被指定至一個特定之人員。依此方式，其係達成該被取得之健康資料係不能夠被指定至一個特定之個人而無該個人之合作及／或准許。爲了給予准許，適當之授權裝置係能夠被實施成該些病患能夠使用，且該些病患係能夠致能舉例而言一個醫師，使用該個別的資料記錄辨識元碼而由一個中央資料庫取得該需要之健康資料。透過本發明，一方面一個用於健康資料記錄之有效率的中央儲存及管理系統係被達成，另一方面，提供防止未獲授權之人員接取個人化之健康資料之非常佳之保護。

於一個根據本發明之申請專利範圍第 2 項之一個進一步的觀點，該取得一個個別的健康資料記錄所需之該資料

記錄辨識元碼係包含一個儲存於一個電子病患卡上之病患卡碼，以及一個由該病患輸入之一個病患辨識碼。因此，取得資料係需要透過該病患分配之電子病患卡及該病患之他／她之病患辨識碼之輸入兩者。因此，資料取得係藉由該病患之一個雙重保護之合作而受到保護。

於一個根據本發明之申請專利範圍第 3 項之一個進一步的觀點，該資料記錄辨識元碼係包含一個儲存於一個電子病患卡上之病患卡碼，以及舉例而言一個醫師之健康專家之辨識碼，該健康專家之辨識碼係辨識請求該資料且調整存取該個別的健康專家被授權之該健康資料之該特定的部分之健康專家。藉由需要牽涉到該治療之該健康專家之額外的碼，該系統係能夠檢查是否該請求之健康專家係獲得授權且保存該請求之記錄。哪一個人員係已經請求何資料及何時？本發明之申請專利範圍第 3 項係包含該健康專家之該辨識碼係儲存於一個特定的健康專家卡上。該健康專家之該辨識卡係包含具有或者不具有被一個健康專家所施加之該健康專家之一個個人辨識碼之該卡碼。

於一個根據本發明之申請專利範圍第 4 項之一個進一步的觀點，該資料記錄辨識元碼之轉移及／或由該中央資料庫取得之該健康資料的轉移係以加密或者編碼模式而執行。此係提供該資料記錄辨識元之未獲授權中途截取及／或由該資料庫取得而來之該健康資料之保護，且因而進一步增加該資料保護。

於一個根據本發明之申請專利範圍第 5 項之一個進一

步的觀點，該系統係提供該終端裝置之該終端使用者，特別是例如於其辦公室或者實驗室中之該醫師之該健康專家，時間上之有限授權，以上載其之病患之新的或者更新過之健康記錄至該中央資料庫。然而，如此之請求僅係於一個成功之授權之程序之後被處理，以登錄及接取該被請求之資料，其中，該病患必須參與且其係根據該特定之資料記錄辨識元。程序係致能牽涉到該治療之該健康專家，以於看見該病患之後某一個期間輸入新的健康資料至一個中央資料庫，舉例而言一些週或者月，且該病患不需要於該資料被輸入時出現。

於一個根據本發明之申請專利範圍第 6 項之一個進一步的觀點，該電子病患卡係包含辨識該人員之一個圖像或者生物資訊元件。牽涉於該治療中之該健康專家係能夠將該圖像（或者生物資訊元件）及呈該現卡給他之該人員，以證明該人員之身份。此係避免該卡之濫用。

於一個根據本發明之申請專利範圍第 7 項之一個進一步的觀點，該系統係包含一個於該中央系統中之一個匿名化系統。該電腦系統係實體上與該中央健康記錄資料庫分離，且係該些資料庫無線上之連結。該匿名化系統係一方面係包含一個人員辨識資料之匹配表，且另一方面包含資料記錄辨識元碼。爲了輸入一個個別的病患之健康資料至該中央資料庫之內，較佳的情況爲，該健康資料係被編碼／加密，且與該個別的人員辨識資料一起傳送至該匿名化系統。如此之人員辨識資料可以被使用作爲非公開的，類

似密碼辨識元，保險號碼等等。然後，該匿名化系統係以該對應之資料記錄辨識元碼取代該人員辨識資料，且提供該碼及用於離線傳輸之該被接收之健康資料至儲存用於後來之取出之個別的中央健康記錄資料庫。健康資料之取出係能夠，而大部分不需要，以該資料記錄辨識元不離開該中央位置之相同方式作處理。由該健康記錄資料庫而來之該匿名化系統之該實體分離係使得對於未獲授權之人員而言，獲得對於指定給個別病患之健康記錄之接取係不可能的，即使其可能成功侵入一個資料庫之中。

於一個根據本發明之申請專利範圍第 8 項之一個進一步的觀點，一個閘道器系統係被設定成與該中央位置內之該匿名化系統實際上分離。該使用者側之終端機係能夠以線上方式連接至該閘道器系統。較佳的情況為，該閘道器系統係接收編碼過／加密過之健康資料及由該使用者偵終端機而來之該對應之人員辨識資料，且透過上載而於上述時間限制內傳送而用於更新。該閘道器系統係實施所有各種資料合理性、接取允許及病毒（特別是木馬病毒）等等之檢查，必要時清除該些資料，且然後提供該資料用於離線傳輸至該匿名化系統。以此方式，該匿名化系統係實際上完全與該使用者側之終端機及對應之資料網路分離。此係確保指定該人員辨識資料至該資料記錄辨識碼之該檔案表對於未獲授權之線上接取者而言係完全保密。

於一個根據本發明之申請專利範圍第 9 項之一個進一步的觀點，一個建檔於該中央資料庫內之該病患的個人健

作為一個健康資料記錄及一個個別指定之資料記錄辨識元碼。該健康資料可以包含電子處方，醫師之信，實驗數據，X 光照片等等。該資料庫可以包含於該中央或者／及去集中化位置中之數個實體資料庫，且特定之記錄甚至可以以去集中化之方式而僅儲存該資料被儲存於何處及如何接取記者會於該中央資料庫之部分的資訊（舉例而言，X 光照片可以以去集中化之方式儲存於其已經被準備好之醫院中，且該 X 光照片被儲存之資訊以及該對應之醫師的信將建檔於該中央資料庫中）。該資料記錄辨識元碼係以單獨由其知識而參考該病患之身份係不可能之方式而組成。以此方式，係能夠確保一個未獲授權之人員係不能夠辨識哪一個病患之健康資料係被儲存及哪一個資料係屬於一個特定之病患，甚至在他可能能夠非法請求由該資料庫（4）而來之資料。

該對於特定之病患的取出之健康資料之指定係需要該個別的病患之主動合作，除了下述之該系統具有一個特定的設計之緊急情況之外。為了此目的，如示於第 1 圖之於該基本版本中之該系統係包含用於每一個病患之電子病患卡（5）。於此卡中，該病患卡碼（5 a）係被儲存。該碼亦能夠被敘述為該病患之卡號。為了資料保護之更進一步改進，作為該系統之一個使用者之每一個病患係接收一個個人辨識碼及僅為該病患自己知道之該病患辨識碼（PIN）。該病患辨識碼係有助於確定該卡之使用者係真正為該卡之擁有者，且確保該取出之健康資料係指該個別的病患，

亦即，一個病患卡（5）之未獲授權的擁有係不能致能該健康資料記錄之請求。不使用或者除了如此之一個病患辨識卡，亦能夠使用一個替代之保密地辨識一個人員之碼；舉例而言，一個包含特別的生物資訊之個人資料的碼。

該卡號（5a）及該病患辨識碼之形式係分別產生該資料記錄辨識元碼（data record identifier code, DIC）及該適當的健康資料記錄，該適當的健康資料記錄係儲存於該中央資料庫（4）中且其係於一個成功的資料取出期間被傳送。爲了該目的，該病患卡（5）係被插入至一個使用者側之終端裝置之中，例如於該醫師之辦公室之中。此外，該病患係輸入他／她之病患辨識碼。該終端裝置係傳送卡號碼（5a）及病患辨識碼，以分別形成及產生該病患之資料記錄辨識元碼，至該中央系統（3），以請求該個別病患之健康資料記錄。

該中央系統（3）係產生該資料記錄辨識元碼，且以該資料庫來源電腦（4）檢查是否該被傳輸之資料記錄辨識元碼係與該儲存之資料記錄辨識元碼之一係相符，且於發現相符之情況下，傳送該對應之健康資料記錄（資料記錄辨識元碼，GD）至該詢問之終端裝置（1）。即使該資料轉移係由一個未獲授權之人員所監視，他／她將不能夠指定該健康資料（資料記錄辨識元碼）至一個特定之人員，因爲其係不包含任何人員辨識資訊。甚至假如一個未獲授權之人員係略微捕捉該資料記錄辨識元碼且接取屬於該特定資料記錄辨識元碼之該健康資料，他或她將不能決定

該健康資料屬於誰，因為該資料記錄辨識元碼係不包含人員辨識資料。

對於一個未獲授權之人員而言，即使該未獲授權之人員係闖入位於牽涉到該治療之類似醫師或者藥劑師之該健康專家處之該終端裝置（1）時，亦係不可能破解該資料之匿名，因為該系統（1）係不知道該病患之卡號（5a）亦不知道該病患之病患辨識碼。該病患卡（5）係能夠於請求之下而透過舉例而言一個信用中心被分配，該信用中心係為一個授權發出保密之認證之機構，諸如一個健康保險或者某些公立機構。因此，該用於病患資料之資料處理系統對於防止未獲授權之資料接取係具有足夠之保護。如果有需要，該資料保護措施進一步能夠於下文中所敘述之方式實施。

舉例而言，該病患卡能夠包含一個個人辨識圖像（5b），使得牽涉到該治療之該健康專家（例如該醫師）係能夠檢查是否事實上由該病患呈現給該健康專家之該卡（5）係為該病患本人的，其係能排除濫用及誤用。或者除了一個照片之外，其他安全的辨識措施係能夠被應用至該卡，諸如生物資訊資料。

第2圖係顯示第1圖之該系統之一個變化形式。於此情況下，牽涉到該治療之該健康專家（例如該醫師）係具有他或者她自己之健康專家卡（6），該自己之健康專家卡（6）係包含一個健康專家辨識碼（6a），且可以請求由該健康專家而來之一個額外的個人病患辨識碼。假如病

患資料係被請求由該中央資料庫（4）而來，則該病患卡及該健康專家卡兩者係被插入該終端裝置之中。除了該病患辨識碼（5）、病患辨識碼加上該健康專家辨識碼（6 a）及健康專家個人辨識碼係較佳地以編碼／加密之形式被傳送至該中華系統（3）之外，該請求係如敘述於第1圖而處理。透過該措施，其係能夠監視該系統之哪一個使用者、醫師或者其他健康專家（藥劑師，健康保險等等）係已經於何時點請求何資料。此外，健康專家能夠根據何種資料其係真正需要而被給予有差別的資料之接取。舉例而言，藥劑師，醫師或者健康保險係需要不同的資料。該系統係不僅允許資料保護，亦允許該個人病患之最佳化的私密保護。

於兩個不同的形式中（第1及2圖），較佳的情況為，透過該線上連結（2）之資料轉移係以編碼／加密之方式產生，雖然並不一定需要如此。較佳的情況為，該詢問之碼資料（5 a，病患辨識碼，6 a，健康專家個人辨識碼）的轉移及該取得之健康資料係被加密／編碼。為了該目的，傳統之密碼技術係能被使用。

對於此應用而言，一個具有非常高資料保護特性之特別有效率之方法係為於該電子病患卡（5）中實施一個加密演算法（5 c）（見第2圖之虛線部分）。於此情況下，該病患卡（5）係被設計成使得於插入該裝置（1）之後，其係分別讀取由該病患所鍵入之該病患辨識碼（但不儲存該病患辨識碼），且當可使用時，讀取由該健康專家所

鍵入之該健康專家辨識碼（6 a），該健康專家係插入其健康專家卡且可能鍵入其個人辨識碼。然後，該加密演算法（5 c）係舉例而言使用一個隨機產生之碼，而產生一個加密過／編碼過之資訊，該資訊係包含該病患卡號（5 a），該個人辨識碼及該健康專家辨識碼（6 a），且可能其個人辨識碼，全部皆為加密／編碼之形式且例如一個亂數。僅該加密過／編碼過之資訊係透過終端裝置（1）而傳送至該中央系統（3）。一個對應之解密演算法係於該中央系統（3）中實施，該演算法係解密該被傳送之資訊。該解決方案係具有下列優點：該病患之卡號（5 a）係能夠以不可能由該卡（5）讀取該卡號之方式實施。因此，該卡號（5 a）係維持一個完整之保密（相同之方式係可以應用至該個人辨識碼，或者該個人辨識碼係能夠被該中央系統所檢查，而省略藉由入侵該病患卡而讀取該個人辨識碼之任何機會）。透過該設計，該病患卡號係不能夠被該終端（1）（或者其他裝置）所讀取，且透過該終端（1）之一個病患卡號之未授權截取係維持不可能。此外，係不可能藉由監視由該終端（1）至該中央系統（3）之資料記錄辨識元碼的資料轉移而知道一個病患之卡號。

對於該被請求之健康資料之轉移而言，舉例而言，一個傳統之加密系統係能夠被使用，其係具有一個用於該使用者之保密碼（私有之密鑰）及一個用於該中央系統之等定的“公共密鑰”。於此情況下，所有健康專家（6 a）及以匿名形式之該資料記錄辨識元碼之所有被授權之終端裝

置（1）之該些碼／公共密鑰係出現於該中央系統（3）之內。於一個請求之情況下，該中央系統（3）係使用該特定之公共密鑰而傳送該加密過／編碼過之健康資料至該提出請求之終端裝置（1）。於該終端裝置（1）處，該資料係藉由使用該個別的保密私有密鑰而解碼。該特定的私有密鑰可以包含該病患／病患卡（5）及該健康專家／健康專家卡（6）之該保密密鑰。於該保密程序之後，該健康資料係能夠被讀取且被分析。

第3圖係圖示關於用於由一個終端裝置（1）至該中央系統之該中央資料庫之新的健康資料之輸入的高度資料保護的非常良好之解決方案之相關元件。於該解決方案中，該中央系統（3）係包含該資料庫（4），一個匿名化系統（亦稱為假名系統）（7）及一個入口伺服器（8）。該解決方案之特徵係為：該匿名化系統（7）係實質上與該資料庫（4）及該入口伺服器（8）分離。因此，由入口伺服器（8）至匿名化系統（7）及由該匿名化系統（7）至該資料庫（4）之資料轉移係分別透過一個特定之離線連結（10）而處理，例如傳統之批次或者固定處理或者即時離線模式（接收伺服器係切斷至該傳送伺服器之線上連結，且檢查該接收到之資料，然後，建立至相關中央系統單元之連結，且傳送資料）。該系統之設計係防止對於該匿名化系統（7）之任何未獲授權的線上接取。

該匿名化系統（7）之主要任務係為於包含個人辨識資料及可能的健康資料之每一個請求中，以該個別的病患

之資料記錄辨識元碼取代該個人辨識資料。該目的係為提供完全的匿名化，匿名化之健康資料，以用於在該資料庫（4）中建檔。於一個未獲授權之請求的情況下，該匿名化資料係能夠使用該資料記錄辨識元碼而被指定至該正確之病患。

於該系統之一個基本形式中，一個病患之新的健康資料及辨識該病患之資料係被該健康專家由該健康專家之終端（1）透過一個線上連結（9）而傳送至該中央系統（3）。該線上連結（9）能夠為與用於資料請求或者該網路之任何其他連結相同之連結（2）。該入口伺服器（8）係接收該個人辨識資料及健康資料，且提供該資料以用於至該匿名化系統（7）之離線輸出。該匿名化系統（7）係接收該離線轉移之資料，且如上所述，以該個別病患之該資料記錄辨識元碼取代個人辨識資料，以提供該健康資料及該資料記錄辨識元用於進一步之轉移。為了此目的，一個個別轉換之指定表係於該匿名化系統（7）中實施，該指定表係指定個人辨識資料（姓名，出生年月日等等）至該個別病患之該個別的資料記錄辨識元碼。資料及該資料記錄辨識元碼係以一個允許個人辨識資料之自動刪除及以資料記錄辨識元碼取代該個人辨識資料之格式而轉移。於下一個步驟中，該健康資料及碼係透過離線連結（11）而被轉移至該資料庫（4），且於該資料庫中建檔。用於一個特定病患之該健康資料係能夠透過一個獲得授權之請求而由該中央資料庫（4）被取出。如此之請求係必

須包含該正確之資料記錄辨識元碼之轉移。

爲了於僅於一段期間檢查其病患之後給予一個健康專家在該中央資料庫（4）中將健康記錄建檔之機會，於一個具有進一步增加之資料保護之該系統係被建構成使得該中央系統（3）係該健康專家請求同時該病患係存在之該健康資料，較佳地，一個加密過之形式之個人資料入口許可係允許該健康專家於該檢查之後之一有限期間將該病患之健康資料建檔。該資料入口許可係於一個可調整期間爲有效的，舉例而言幾週或者幾個月。其給予一個健康專家轉移其病患之健康資料之機會，即使該病患係不以敘述於第3圖之方式出現至該中央資料庫（4）且於該中央資料庫（4）中建檔。

此程序係不同於如敘述於第3圖中之其基本版本之該資料上載。該健康資料係不與該個人辨識資料一起傳送，而係與該個別之健康專家的病患之該個人資料入口許可一起由終端裝置（1）傳送至入口伺服器（8），且於入口伺服器（8）以離線模式傳送至匿名化系統（7）。使用一個表，系統（7）係以該病患之資料記錄辨識元碼取代被時間所限制之該資料入口許可。於該健康專家於其許可已經到期之後想要上載健康資料至該中央資料庫（4）之情況下，此係必須於另一個安全程序之中執行，舉例而言藉由以電子郵件傳送該健康記錄，於該情況下，其係在該中央系統（3）之中被數位化，或者透過另一個高度保護之轉移模式。

或者除此之外，爲了給予健康專家用於上載健康資料至該中央資料庫（4）之時間限制，敘述於第3圖之程序係能夠被修改，以透過線上連結（9）藉由傳送加密過／編碼過之資料而達成一個更高之資料保護，舉例而言藉由敘述於第1及2圖之該些演算法之一而執行。

到目前爲止所述之該系統設計係僅於該個人病患出現時允許一個健康專家由該中央資料庫（4）取出資料。爲了使該必須之健康資料於任何緊急情況下可以由一個一個健康專家所使用，該系統係包括一或數個適當的緊急措施。

於一個第一緊急措施中，於緊急情況下通常需要一個病患之如此健康資料係用於直接取出而儲存於該電子病患卡（5）之內，例如血型，過敏，目前所服用之藥物／藥品，於緊急期間相關之診斷，等等。一個健康專家僅能夠於緊急情況下藉由該病患卡而接取相關之資料。

作爲一個進一步之措施，該系統係能夠包含一個緊急呼叫中心，其係具有接取儲存於該中央資料庫（4）中之每一個病患的該健康資料之至少一個緊急相關之部分。於一個緊急之事件之下，該健康專家必須對於該呼叫中心之代理者驗證該健康專案之身份。爲了此目的，每一個健康專家係接收一個個人的驗證碼。於驗證之後，他係接收該必須之緊急健康資料。爲了維持足夠的資料保護，該病患必須同意事先接取其健康資料之緊急權利係有意義的，舉例而言當該卡發進至該病患時。此外，該病患必須被通知

- 5 病患卡
 - 5 a 病患卡碼
 - 5 b 個人辨識圖像
 - 5 c 加密演算法
- 6 健康專家卡
 - 6 a 健康專家辨識碼
- 7 匿名化系統
- 8 入口伺服器
- 9 線上連結
- 1 0 離線連結
- 1 1 離線連結

(name, date of birth, etc.) but with a DIC which is required for access to health data.

The invention can be used, e.g. for electronic health records.

拾、申請專利範圍

1．一種用於病患資料之資料處理系統，其係包含一個個別病患之個人辨識資料及對應之健康資料，其係包含：

一或數個中央系統，每一個中央系統係具有一個資料庫（4）及

複數個終端裝置（1），其係與該資料庫（4）相連結，以由該中央資料庫（4）取出健康資料及／或用於上載健康資料至該中央資料庫（4），其特徵為：

於該中央資料庫（4）中儲存健康資料 GD 係不指定至諸如姓名、出生年月日等等之人員辨識資料，而係分配一個病患之該健康資料至該對應之資料記錄辨識碼，該資料記錄辨識碼對於資料請求係必要的。

2．如申請專利範圍第1項之用於病患資料之資料處理系統，其中，該資料記錄辨識碼係包含被儲存於一個病患卡（5）中之一個病患卡碼（5a）及一個由該病患輸入之一個個人辨別碼。

3．如申請專利範圍第1或2項之用於病患資料之資料處理系統，其中，該資料記錄辨識碼係包含：一個病患卡碼（5a），其係被儲存於一個病患卡（5）中之一個病患卡碼（5a）；及一個儲存於一個健康專家之卡（6）上之健康專家辨識碼（6a），額外之資料保護係藉由使用用於該病患之個人辨識卡及該健康專家卡而被允許。

4．如申請專利範圍第2項之用於病患資料之資料處

理系統，其中，該資料記錄辨識碼之加密／編碼轉移及／或健康資料之加密／編碼轉移係由該中央資料庫而來或者上載至該中央資料庫。

5．如申請專利範圍第1項之用於病患資料之資料處理系統，其中，一個資料入口碼係具有時間限制，該資料入口碼及該個別的健康資料係被該中央系統（3）傳送至該請求之終端裝置（1），該資料入口碼係給予該提出請求之終端裝置（1）及該健康專家於上載該特定之病患健康資料至該中央資料庫（4）之該起始請求之後之一個有限期間之許可。

6．如申請專利範圍第2項之用於病患資料之資料處理系統，其中，一個包含一個病患辨識圖像（5b）或／及生物資訊資料之病患卡係清楚地辨識該病患。

7．如申請專利範圍第1項之用於病患資料之資料處理系統，其中，該中央系統（3）係包含一個匿名化系統（7），該匿名化系統（7）實體上與該中央資料庫（4）分離，該匿名化系統（7）一方面係包含具有個人辨識資料（姓名，出生年月日，保險號碼，護照號碼等等）之一個分配表，另一方面係包含該對應之資料記錄辨識碼，於該輸入側，該匿名化系統（7）係接收該健康資料及該對應之個人辨識資料，該系統係以該對應之資料記錄辨識碼取代該個人辨識資料，於該輸出側，該匿名化系統（7）係準備該健康資料及該對應之資料記錄辨識碼，以用於在該中央資料庫（4）中建檔。

8．如申請專利範圍第7項之用於病患資料之資料處理系統，其中，該中央系統（3）係包含一個入口伺服器（8），該入口伺服器（8）係實體上與該匿名化系統（7）分離，且該終端裝置（1）係連接至該入口伺服器（8），以用於線上資料轉移，該入口伺服器（8）係提供用於至該匿名化系統（7）之離線轉移的資料。

9．如申請專利範圍第2項之用於病患資料之資料處理系統，其係包含一個病患卡，用於該個別病患之該健康資料之一個可選擇的部分係被儲存於該病患卡之上，且能夠被獲得授權之健康專家所接取，例如於緊急情況下，藉由從該卡直接讀取。

10．如申請專利範圍第1項之用於病患資料之資料處理系統，其中，其係包含一個緊急呼叫中心，該緊急呼叫中心係被授權由該中央系統取出每一個病患之該健康資料的至少一個緊急相關的部分，該緊急呼叫中心係包含對於健康專家授權之裝置，以使該些健康專家由該緊急呼叫中心接收緊急健康資料。

I254233

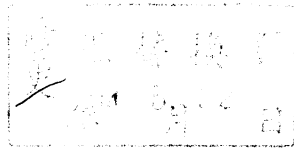
拾壹、圖式

如次頁

陸、(一)、本案指定代表圖爲：第____圖

(二)、本代表圖之元件代表符號簡單說明：

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

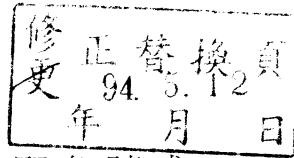


康資料之一個相關部分亦係儲存於該病患卡之上，以用於有規則及受限制之接取。此係提供牽涉於該治療中之一個健康專家，於該病患係不能夠允許接取該中央資料庫之緊急情況下，有機會透過該卡而知道一個病患之該健康狀態。

於一個根據本發明之申請專利範圍第 10 項之一個進一步的觀點，該系統係提供一個緊急呼叫中心。該呼叫中心係具有接取該中央資料庫之授權，以於該病患係不能夠自己允許接取其健康資料之緊急情況下請求特定之資料，且提供如此之資料至牽涉到該治療之該健康專家。該健康專家必須使用適當的辨識裝置而對於該呼叫中心辨識自己。

【實施方式】

第 1 圖係示意地圖示請求由用於病患資料之一個資料處理系統而來之資料及上載資料至一個用於病患資料之資料處理系統所需之相關元件。該系統係包含一個典型地包含許多使用者側之終端裝置之資料網路。通常，巨大數量之使用者側終端裝置（1）係透過線上連接而連接至該中央系統（3）。於第 1 圖中，這些終端裝置係由一個個人電腦（1）所表示。該中央系統係包含一個作用為一個中央資料庫（4）之來源電腦。假如有需要，具有個別資料庫之許多中央系統係能夠於許多中央或／及去集中化位置中被設定作為去集中化之網路。於該中央資料庫（4）中，一個個別病患之該健康資料係以呼叫模式建檔，而



關於每一個後來的緊急請求。

於該病患卡或者該健康專家之卡係遺失之情況下，這些卡係透過一個傳統之方式而使其無效，例如已知之由信用卡之方式。舉例而言，該擁有者係呼叫該中央系統（3）檢查該呼叫者之授權（例如，透過再呼叫及／或僅為該呼叫者知道之保密資訊），且然後，使該卡無效。

上述之執行係使得本發明提供一個具有所謂的電子健康記錄之病患資料之處理的資料處理系統變成清楚，其係為符合如此之資料所需之相當高的資料保護標準。

【圖式簡單說明】

（一）圖式部分

本發明之有優點之實施方式係呈現於下列圖式中，其中：

第 1 圖係為一個顯示用用於處理該病患資料之一個系統而來之資料請求的相關元件之示意方塊圖；

第 2 圖係為用於第 1 圖之一個替代系統之一個示意方塊圖；及

第 3 圖係為一個顯示用於輸入／上載資料至根據第 1 圖及第 2 圖之用於處理病患資料的系統。

（二）元件代表符號

- 1 終端裝置
- 2 線上連結
- 3 中央系統
- 4 中央資料庫

肆、中文發明摘要

本發明係關於用於一種病患資料的處理之資料處理系統，該病患資料係包含每一個病患之個人辨識資料及對應之健康資料。其係具有一個中央系統（3），該中央系統（3）係包含一個儲存該健康資料之中央資料庫（4），且具有複數個終端裝置（1），該複數個終端裝置（1）係與該中央系統（3）連接，以用於向該中央資料庫請求健康資料及／或用於輸入健康資料至該中央資料庫。根據本發明，健康資料係儲存於該中央資料庫（4）中，而健康資料係不指定至個人辨識資料（姓名、出生年月日等等），而係分配一個病患之該健康資料至該對應之資料記錄辨識碼，該資料記錄辨識碼對於接取資料係必要的。本發明係能夠被使用於例如電子健康記錄。

伍、英文發明摘要

The invention refers to a data processing system for the processing of patient data, which includes person identifying data of a respective patient and corresponding health data (GD), with a central system (3), which includes a database (4) storing the health data, and with terminal devices (1), which are connected with the central system for the request of health data from the database and /or for the input of health data into the central database.

According to the invention, health data is stored in the central database without assignment to person identifying data

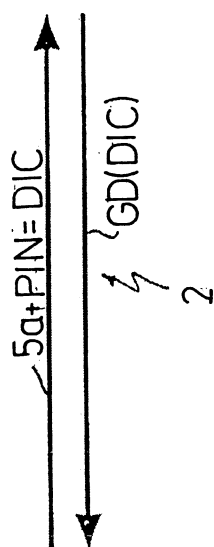


圖
1
集

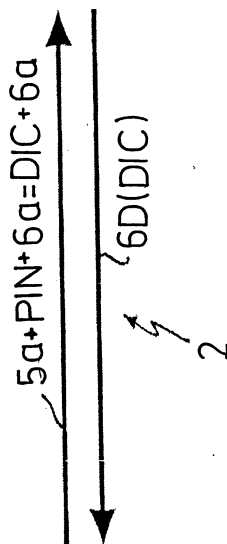
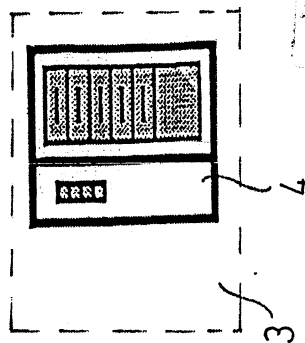
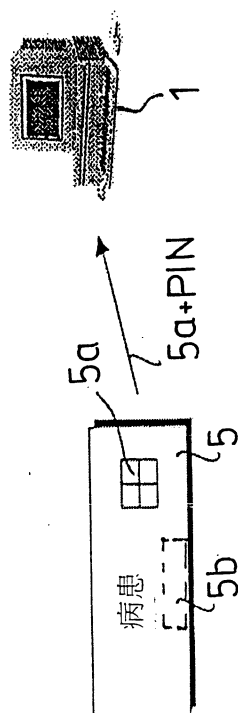
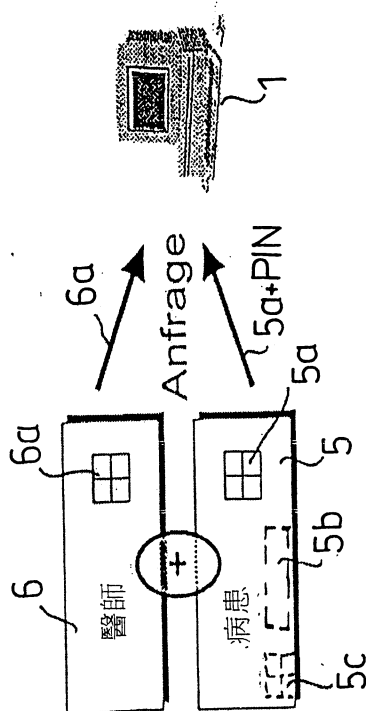


圖
11
紙



94. 5. 12

修正替换頁
年 月 日
修史

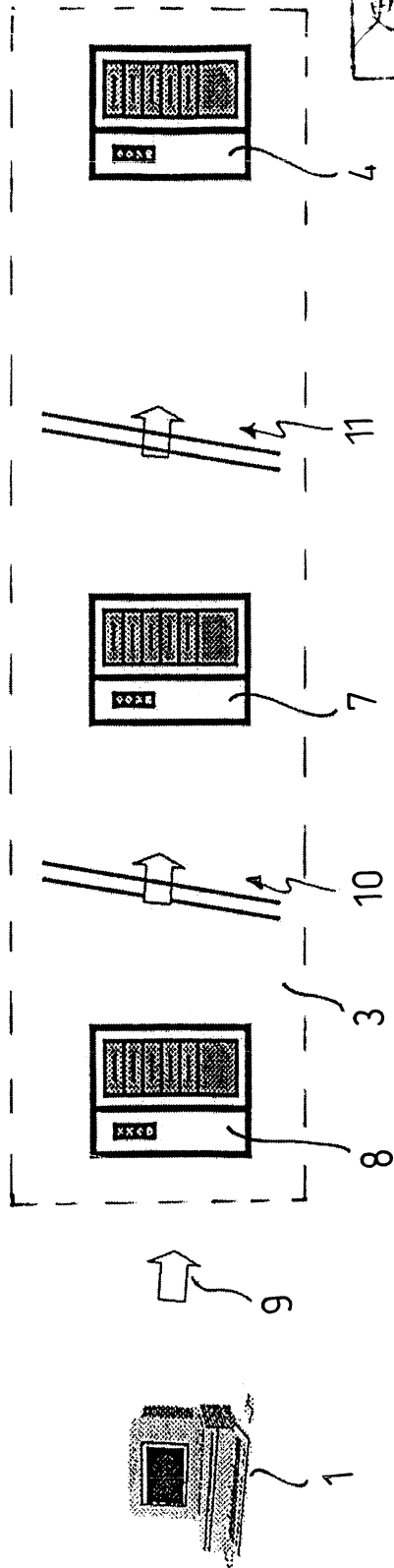


圖
111
築