



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: 2014138065, 04.12.2012

Приоритет(ы):

(30) Конвенционный приоритет:
22.02.2012 DE 10 2012 202 701.7

(43) Дата публикации заявки: 10.04.2016 Бюл. № 10

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 22.09.2014(86) Заявка РСТ:
EP 2012/074334 (04.12.2012)(87) Публикация заявки РСТ:
WO 2013/124014 (29.08.2013)Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, строение 3,
ООО "Юридическая фирма Городиский и
Партнеры"

(71) Заявитель(и):

СИМЕНС АКЦИЕНГЕЗЕЛЛЬШАФТ (DE)

(72) Автор(ы):

**ФРИЗЕ Томас (DE),
ГОССЛЕР Томас (DE)****(54) СПОСОБ ОБРАБОТКИ ОТНОСЯЩИХСЯ К ПАЦИЕНТУ КОМПЛЕКТОВ ДАННЫХ****(57) Формула изобретения**

1. Способ обработки относящихся к пациенту комплектов данных, которые содержат медицинские данные и доверительные данные пациента в виде открытых данных, в котором

доверительные данные пациента каждого относящегося к пациенту комплекта данных подвергаются обезличиванию (20), за счет чего создаются анонимные относящиеся к пациенту комплекты данных,

с помощью алгоритма из соответствующих доверительных данных пациента каждого относящегося к пациенту комплекта данных генерируют проверочные данные и включают (18) в соответствующий относящийся к пациенту комплект данных,

анонимные относящиеся к пациенту комплекты данных с проверочными данными передают (22) в распоряжение в распределенной компьютерной архитектуре (2),

в клиентском компьютере (24), который соединен с распределенной компьютерной архитектурой (2), в рамках обработки определенного относящегося к пациенту комплекта данных задают доверительные данные выбранного пациента, и с помощью алгоритма из этих заданных доверительных данных пациента создают (26) данные запроса, и

инициируют функцию защиты, когда проверочные данные определенного относящегося к пациенту комплекта данных не совпадают с данными запроса выбранного пациента.

2. Способ по п. 1, в котором доверительные данные пациента каждого относящегося к пациенту комплекта данных разделяют (16) на данные кодирования и остальные доверительные данные пациента, все доверительные данные пациента каждого относящегося к пациенту комплекта данных обезличивают (20), за счет чего создают анонимные относящиеся к пациенту комплекты данных, однако с помощью алгоритма лишь из соответствующих данных кодирования каждого относящегося к пациенту комплекта данных генерируют проверочные данные и вводят (18) в соответствующий относящийся к пациенту комплект данных, анонимные относящиеся к пациенту комплекты данных предоставляются в распоряжение в распределенной компьютерной архитектуре (2), в клиентском компьютере (24), который соединен с распределенной компьютерной архитектурой (2), в рамках обработки определенного относящегося к пациенту комплекта данных задают данные кодирования выбранного пациента и из этих заданных данных кодирования с помощью алгоритма генерируют (26) данные запроса, и иницируют функцию защиты, когда проверочные данные определенного относящегося к пациенту комплекта данных не совпадают с данными запроса выбранного пациента.
3. Способ по п. 1, в котором алгоритм задан однонаправленной хеш-функцией.
4. Способ по п. 1 или 2, в котором множество анонимных относящихся к пациенту комплектов данных с проверочными данными из распределенной компьютерной архитектуры (2) содержат данные индикации для отображения на клиентском компьютере (24).
5. Способ по п. 1 или 2, в котором множество относящихся к пациенту комплектов данных содержат данные изображения, и в котором из данных изображения одного из этих относящихся к пациенту комплектов данных в распределенной компьютерной архитектуре (2) создают (28) данные индикации для отображения на клиентском компьютере (24).
6. Способ по п. 4, в котором данные индикации и проверочные данные определенного относящегося к пациенту комплекта данных сначала поступают в распоряжение в клиентском компьютере (24), в котором затем эти проверочные данные сравнивают (30) с данными запроса, и в котором иницируют функцию защиты, когда проверочные данные не совпадают с данными запроса.
7. Способ по п. 5, в котором данные индикации и проверочные данные определенного относящегося к пациенту комплекта данных сначала поступают в распоряжение в клиентском компьютере (24), в котором затем эти проверочные данные сравнивают (30) с данными запроса, и в котором иницируют функцию защиты, когда проверочные данные не совпадают с данными запроса.
8. Способ по п. 1, в котором проверочные данные включены графически в данные индикации.
9. Способ по п. 4, в котором проверочные данные включены графически в данные индикации.
10. Способ по п. 5, в котором проверочные данные включены графически в данные индикации.
11. Способ по п. 6, в котором проверочные данные включены графически в данные индикации.
12. Способ по п. 8, в котором проверочные данные включены в данные индикации в виде двухмерного штрих-кода.
13. Способ по п. 4, в котором отображение данных индикации воспрещается, когда

инициирована функция защиты.

14. Способ по п. 5, в котором отображение данных индикации воспрещается, когда инициирована функция защиты.

15. Способ по п. 8, в котором отображение данных индикации воспрещается, когда инициирована функция защиты.

RU 2014138065 A

RU 2014138065 A