República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

# (21) PI 0717818-2 A2

(22) Data de Depósito: 13/09/2007
**(43) Data da Publicação: 12/11/2013**
**(RPI 2236)**

***(51) Int.Cl.:***
**G06F 19/00**

**(54) Título:** SISTEMA DE SEGURANÇA PARA REGISTROS MÉDICOS; MÉTODO PARA ACESSO SEGURO DOS REGISTROS MÉDICOS; E SISTEMA PARA ACESSO SEGURO DOS REGISTROS MÉDICOS.

**(57) Resumo:**

**(30) Prioridade Unionista:** 14/09/2006 US 11/522,093

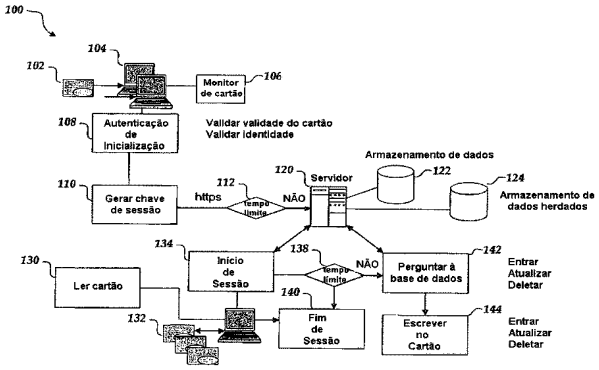
**(73) Titular(es):** Chi-Square Technologies L.L.C.

**(72) Inventor(es):** Robert D. Highley

**(74) Procurador(es):** Araripe & Associados

**(86) Pedido Internacional:** PCT US2007020123 de 13/09/2007

**(87) Publicação Internacional:** WO 2008/033554de 20/03/2008



**"SISTEMA DE SEGURANÇA PARA REGISTROS MÉDICOS; MÉTODO PARA ACESSO SEGURO DOS REGISTROS MÉDICOS; E SISTEMA PARA ACESSO SEGURO DOS REGISTROS MÉDICOS".**

O presente pedido está sendo depositado em 13 de setembro de 2007 como pedido de patente internacional nos termos do PCT, em nome de Robert D. Highley, cidadão dos Estados Unidos e depositante/inventor nomeado para todos os países designados. Este pedido reivindica prioridade do pedido de patente Número U.S. 11/522.093, depositado em 14 de setembro de 2006.

Antecedentes da invenção

Os sistemas de cuidados com a saúde existem, com freqüência, independentemente e têm sido descritos como " uma confederação de indústrias caseiras". A população para a qual os sistemas de cuidados com a saúde existem é móvel e os cuidados médicos são prestados episodicamente, freqüentemente através de sistemas de atendimento (como prestadores de cuidados médicos), o que torna difícil o fornecimento da continuidade real dos cuidados com o uso de sistemas convencionais. Os registros médicos não estão sempre disponíveis no local dos cuidados, mesmo dentro de um único sistema de atendimento. Os registros médicos não estão, usualmente, prontamente disponíveis para um determinado sistema quando os cuidados foram previamente prestados fora de tal sistema. De modo adicional, os registros médicos nunca estão, usualmente, disponíveis para socorristas de primeira linha, especialmente em situações de emergência.

Os registros médicos são, de modo típico, de base institucional e são transferidos, normalmente, entre as instituições de acordo com o mandato HIPAA (Ato de Responsabilidade e Privacidade de Informações sobre Saúde) restrito. Com freqüência, faltam partes do registro e esses têm que ser "re construídos". Os registros reconstruídos freqüentemente possuem lacunas significativas e o simples preenchimento dos espaços em branco com a "situação mais provável" muitas vezes pode criar erros, os quais podem se multiplicar fazendo com que erros pequenos, porém consideráveis, repentinamente se tornem erros letais em potencial. Portanto, o sistema convencional também fragmente, com freqüência, os dados médicos, o que cria omissões e difunde erros. O Instituto de

Medicina estima que mais de 98.000 pessoas morrem a cada ano devido a erros médicos e isso poderia ser evitado.

As emergências públicas recentes, como furacões de categoria 5 e atos coordenados de terrorismo, têm demonstrado as conseqüência s dos sistemas convencionais devido a, por exemplos, linhas de comunicação avariadas e/ou circuitos de comunicação sobrecarre gados.

Sumário da invenção

A presente revelação fornece modalidades exemplificativas da invenção, a qual é definida pelas reivindicações conforme aqui citadas. Em diversas modalidades, um sistema de registros médicos é revelado que disponibiliza, de modo resistente, oportuno, preciso e seguro, os registros médicos necessári os para prestadores de cuidados médicos arbitrár ios, porém autorizados, de uma maneira interoperativa, mesmo durante os momentos de desastres públicos e emergências. O sistema de registros médicos conectaria pacientes, provedores, farmácias, clínicas, hospitais, pagantes e produtores através de uma rede privada segura que opera em tempo real e pode operar sem a grade de energia ou sem Internet no caso de desastres naturais ou causados pelo homem.

O sistema de registros médicos fornece uma solução tecnológicae processos comerciais que podem conectar um indivíduo autorizado em tempo real, com ou sem conectividade, como àquela fornecida pela Internet. Um método e um aparelho para um sistema de registros médicos global portát il (GPMR) é revelado e fornece uma conectividade universal com ou sem a Internet às pessoas em questão em locais arbitrár ios.

Em uma modalidade, um cartão inteligente fornece um meio portáti l destinado a portar dados de emergência médicas e fornece um acesso de segurança a uma rede privada virtual (VPN). A VPN fornece uma transmissão segura de dados criptografados entre os "seis P's" (pacientes, provedores, pagantes, planos, produtos farmacêuticos e produtores). Normalmente não é possível entrar na VPN sem um cartão inteligente emitido por um certificado de autoridade. Todas as trocas de informações podem ser acompanhadas a fim de garantir a privacidade do paciente e a conformidade com o HIPAA. Um modelo de ASP (páginas do servidor ativas) pode ser usado para

entregar os conteúdos dos registros médicos e conectar os registros do cartão inteligente para a VPN e para os servidores da base de dados com a finalidade de completar o sistema.

O sistema de registros médicos pode fornecer um registro longitudinal dos dados originais com o decorrer do tempo e por meio dos sistemas de atendimento. Em funcionamento, cada instituição registra o ocorrência atual de cuidados e adiciona os dados originais a um registro longitudinal em andamento. O paciente leva consigo um cartão inteligente sem dados de núcleo para usos emergenciais e um enlace (como um URL) a um servidor, onde todo o seu registro médico é alojado. Dessa maneira, um acesso universal é fornecido para um registro médico portá til em tempo real totalmente integrado e ultra-seguro que agrega os dados originais com o decorrer do tempo e por meio dos sistemas de atendimento. A integração e a conectividade diminuirá, de modo típico, os erros médicos, aperfeiçoará os cuidados médicos e reduzirá os custos. Ademais, os cartões inteligentes podem ser configurados para transferir por download as informações pertinentes, como as informações demográficas, para qualquer formulário ou anotação na rede da ASP.

Breve Descrição dos Desenhos

As modalidades não-limitantes e não-exaustivas são descritas com referência aos desenhos a seguir.

A Figura 1 é um diagrama lógico que ilustra um sistema de segurança de acesso duplo para registros médicos.

Descrição detalhada

Diversas modalidades serão descritas em detalhes com referência aos desenhos, onde os números de referência similares representam as partes similares e conjuntos no decorrer de todas as vistas. A referência a diversas modalidades não limita o escopo da invenção, a qual é limitada somente pelo escopo das reivindicações anexadas à mesma. Ademais, quaisquer exemplos estabelecidos nesse relatório descritivo não têm a intenção de limitação e simplesmente estabelecem algumas das muitas modalidades possíveis para a invençã o reivindicada.

Ao longo do relatório descritivo e das reivindicações, as expressões a seguir

possuem, ao menos, os significados explicitamente associados, a menos que o contexto indique o contrár io com clareza. Os significados identificados abaixo não têm a intenção de limitar as expressões, porém meramente fornecem exemplos ilustrativos para uso das expressões. O significado de "uma" e "a" pode incluir a referência tanto ao singular quanto ao plural. O significado de "em" pode incluir "em" e "sobre". A expressão "acoplado" pode significar uma conexão direta entre os itens, uma conexão indireta através de um ou mais intermediários, ou uma comunicação entre itens de uma maneira que não constitua uma conexão.

O Registro Médico Global Portáti l (GPMR) refere-se a um registro de microchip do cartão inteligente que pode conter, por exemplo, mais de 50 páginas de dados de núcleo (dados demográficos, informações de contato, alergias, informações de seguro de saúde, crescimento e desenvolvimento, histórico social, histórico familiar, lista de medicações, lista de problemas, dispositivo implantáveis, preferências de segurança, preferência de HIPAA, testamento em vida, certidão de nascimento e similares) que podem ser lidos diretamente do cartão (quando, por exemplo, o registro médico de núcleo pode ser acessado somente desconectado). Quando a WAN ou a conexão com a Internet pode ser estabelecida (por exemplo, quando o registro médico de núcleo está conectado), um localizador, como um código de URL, armazenado no cartão pode direcionar o usuário ao servidor, onde o registro médico completar está armazenado. (Portanto, o GPMR fornece um acesso desconectado limitado aos dados médicos de núcleo armazenados no cartão em qualquer emergência onde a Internet não está disponível. Um enlace de URL fornece registros médicos conectados em tempo real de modo que os indivíduos em questão podem ser conectados através de uma rede segura). O registro de Web refere-se a um registro médico completo (laboratórios, raios-X, anotações de procedimento, etc.) armazenado em um servidor administrado por um Sistema de Informações Clínicas (CIS) acessado pela Internet, por exemplo.

O Sistema de Informações Clínicas (CIS) é uma aplicação de software que lança, registra, armazena e recupera registros a partir do repositório da base de dados. Sistemas bem conhecidos são HBOC, OASIS, EPIC, Cerner, IDX/GE, PHAMIS, Last Word e similares.

O Ato de Responsabilidade e Privacidade de Informações sobre Saúde - HIPAA é um conjunto de regulamentos federais que decreta as limitações dos registros de integridade e regras que administram o acesso aos registros médicos privados. A legislação indica que o registro médico pertence ao paciente e o acesso a seu registro pessoal pode ser somente acessado com a permissão e a direção do paciente ou seu guardião designado. Portanto, o individuo detém e controle o uso de seu registro pessoal.

A Segurança de Acesso Duplo (DAS) refere-se a um método para o acesso seguro aos registros médicos. O acesso a um registro médico portát il exige (ao menos) duas chaves e duas senhas para entrar tanto no registro médico portát il quanto no registro da web. Por conseguinte, o paciente normalmente precisa ter posse fís ica de seu GPMR (o qual contém, ao menos, uma primeira chave). O paciente insere (física e/ou logicamente) o GPMR (o qual está, de modo típico, na forma de um cartão de CPU, como um cartão inteligente) no interior de uma leitora que foi emitida e autenticada pela rede privada e dá permissão para acessar o registro lançando-se uma de duas senhas pré-determinadas (por exemplo, uma senha para o registro regular e uma segunda senha para informações que o paciente pré-selecionou como confidenciais). Quando o paciente é autenticado e a permissão é conc edida, o paciente retirará o cartão tipica mente.

Uma segunda chave e senha são normalmente exigidas por um prestador para entrar no sistema/VPN. O prestador (como um médico) insere seu cartão de identificação de microchip emitido e autenticado pela rede. Um marcador biométrico, como uma impressão digital, também pode ser solicitado. Se o(s) número(s) de segurança do cartão e a biometria são compatíveis com a Identificação do usuário e a senha pré-validada no sistema, o cartão é, portanto, autenticado e o acesso ao registro do paciente será permitido, tipicamente se o paciente der (ou deu de alguma outra maneira) consentimento. (Em primeiro lugar, o prestador ativa tipicamente o sistema para que o paciente possa usar o cartão do paciente para dar o consentimento). O identificador de paciente pode ser um número de mais de 9 dígit os precedido por um código de segurança de 4 dígitos. O identificador também pode ser um número de mais de 9 dígitos precedido por um número (ou outro identificador) do sistema de atendimento no qual o médico é privilegiado. O médico pode ter diversos identificadores no cartão de prestador do

médico. Se os códigos de segurança forem compatíveis, o médico possui permissão implícita para entrar, modificar ou excluir informações do registro armazenado no registro médico do paciente. Se os códigos não são compatíveis, então, a senha do paciente pode ser cedida como consentimento para a liberação das informações médicas. Em diversas modalidades, os marcadores biométricos (como impressões digitais, voz, digitalização de retina e similares) podem ser usados. Se os marcadores biométricos, as senhas e/ou outros códigos de segurança pré-instalados, são compatíveis, o registro pode ser acessado.

As condições adicionais podem ser posicionadas na transação. Por exemplo, os níveis de segurança podem ser selecionados pelos pacientes que se inscrevem no sistema de tal modo que somente partes do registro possam ser acessados (como acesso aberto, um registro regular ou um registro confidencial). Ademais, somente o registro do paciente pode ser acessado. (Em sistemas convencionais, pode ser possível ter acesso a todos os registros em um servidor acessível. Em um sistema de cartão inteligente, normalmente apenas o registro que satisfez todas as exigências de segurança pode ser acessado). Quando o médico retira o cartão de prestador, a sessão é automaticamente encerrada sem um cache (como através do esvaziamento do cachê) a fim de retornar àquele registro (o qual está presente em muitos sistemas convencionais). Isso fornece uma segurança adicional, preserva a privacidade do paciente e protege o médico, por exemplo, das multas JACHO, se houver falha no encerramento de comunicação e informações sensíveis do paciente fiquem no computador à mercê de exposição a transeuntes.

Interoperabilidade funcional: A padronização campo a campo entre os sistemas de atendimento ou os Sistemas de Informações Clínicas têm sido difícil de ser atingida devido aos sistemas proprietários competidores que preferem padronização somente se os mesmos são o padrão. A discussão acerca dos padrão tem tornado a interoperabilidade campo a campo quase impossível de ser atingida. A DAS pode resolver esse problema. Os sistemas de atendimento têm que concordar somente com o uso do mesmo protocolo de segurança para acessar seu CIS. Os cartões inteligentes de prestador podem ser usados para entrar em sessão de diferentes CISs, onde quer que os dados do

paciente estejam localizados e independente do sistema de informações. O Registro Médico Global Portáti l pertence ao paciente (conforme comparado à instituição) e, quando o paciente concede permissão, pode-se fazer o levantamento e pode-se acessar somente daquele registro do paciente para aquela sessão naquele CIS. Isso pode eliminar a disputa entre os estudiosos sobre a estrutura do campo e permite que os registros sejam compartilhados em qualquer CIS em um formato de somente leitura a fim de fornecer uma interoperabilidade funcional.

A interoperabilidade funcional proporciona uma solução funcional para o compartilhamento de dados quando se trata de cuidados médicos sem que se faça necessário um acordo universal sobre os padrões de interoperabilidade. Um prestador privilegiado (que possui uma identidade verificada, que é credenciado por um sistema de atendimento e que é autenticado pela rede privada como um assinante válido atualizado) pode acessar o servidor quando o registro completo da Web do paciente está armazenado com o objetivo de acessar aquelas informações. Por exemplo, o prestador privilegiado pode ler um registro em Illinois e gravar pedidos em seu próprio CIS em Oregon. Um sumário pode ser enviado de volta ao médico em atendimento em Illinois. Os registros podem ser compartilhados, portanto, através dos sistemas de atendimento em tempo real, fornecendo uma continuidade de cuidados médicos de modo que a interoperabilidade funcional seja alcançada.

A Figura 1 é um diagrama lógico que ilustra um sistema de segurança de acesso duplo para registros médicos. O sistema 100 compreende um cartão inteligente (como um cartão de microchip/ cartão de CPU ou, por exemplo, um cartão de memória com ou sem a capacidade de processamento). Os cartões inteligentes podem ser um cartão de prestador e/ou cartão de paciente 132. Aos pacientes seriam emitidos registros médicos 132 do cartão inteligente pela empresa do plano de saúde ou pelo Medicare/Medicaid ou uma agencia de saúde pública ou outro emissor. O emissor normalmente forneceria os dados de identidade a fim de garantir a identidade do portador do cartão.

Os pacientes usariam seu cartão para ter acesso ao sistema 100. No primeiro contato com novos assinantes, diversas perguntas seriam tipicamente feitas a fim de completar seu registro médico (demografia, contato e informações sobre o plano de

saúde, alergias, lista de problemas, procedimentos e cirurgias antecedentes, dispositivos, documentos legais, testamento em vida, condição de código, crescimento e desenvolvimento, incapacidades, vacinas, lista de medicações, etc.). A página de entrada pode ser baseada na Web e preenchida em casa ou em um quiosque (no consultório do médico, do Serviço de Saúde Pública, da biblioteca e similares) que é conectado ao sistema 100. Um URL incorporado ao cartão pode ser usado para encontrar o servidor, o qual foi designado para armazenar todo o registro quando emitido e as transferências por download que lançam dados naquele servidor. A transferência pode ocorrer através de uma Rede Privada acessada por meio de um cartão inteligente que foi autenticado no sistema e pode ser ultra-secreto. Caso a Internet pública seja usada, então, a transferência deve ser criptografada (com o uso de uma camada de soquete segura, por exemplo) a fim se garantir a privacidade do paciente.

Os cartões 132 funcionam como registros médicos portátei s que portam dados de núcleo médicos, legais, financeiros, do seguro de vida e da identidade. Os benefícios da apólicede seguro podem ser armazenados no cartão e usados para adjudicar o seguro diretamente do cartão no local de tratamento. "Dinhei ro" pré-pago armazenado nos cartões pode ser usado para co-pagamentos ou descontos. O verdadeiro acesso aos dados do paciente exige a posse física de um cartão de paciente autenticado 132 e uma senha válida compatível do paciente. Exige, ainda, a posse física de um cartão de prestador vá lido 102 e autenticado por um marcador biométrico (como uma impressão digital, voz, digitalização de retina) e/ou por uma senha armazenada no sistema e criptografada no cartão.

Pode haver, por exemplo, três níveis de segurança determinados pelas preferências individuais armazenadas no cartão (1 acesso aberto, 2 registro regular e 3 informações confidenciais). Quando o cartão é inserido em uma leitora, o acesso aberto fica disponível dentro do limite estabelecido pelo paciente. Caso o paciente queira proteger as informações confidenciais, ele concederá a senha padrão e se ele quiser que o médico tenha conhecimento das informações confidenciais, pode digitar a segunda senha que dá acesso a esses dados. Isso confere uma maior proteção de HIPAA ao paciente e ele controla tanto o acesso como o conteúdo, conforme a intenção original do Congresso.

As leitoras de cartão inteligente nas estações 104 e 136 realizam uma verificação de segurança com a finalidade de garantir a autenticidade do cartão. A rede pode selecionar falsificações com o uso de procedimentos de autenticação. A base de dados (armazenamento de dados 122 e/ou armazenamento de dados herdados 124) é a autoridade de dados e quando acessada de modo conectado faz transferência por download das alterações mais recentes ao registro portát il do cartão inteligente. As informações podem ser sincronizar de modo a atualizar os cartões ou de modo a atualizar a base de dados. Caso haja perda ou roubo do cartão, o mesmo pode ser reemitido a partir do repositório da base de dados.

Os dados nos cartões 132 podem ser normalmente apenas acessados por um "cartão inteligente de prestador" 102 emitido pelo sistema 100. Portanto, se houver a perda de um cartão de paciente, as únicas informações disponíveis a uma leitora leiga seriam aquelas designadas como acesso aberto (nome, número de telefone e endereço para devolução do cartão). Se o paciente preferir, todo o registro pode ser disponibilizado como acesso aberto.

Podem ser emitidos para os prestadores (como RNs, MDs, farmacêuticos e similares) um cartão por meio do sistema de atendimento onde trabalham. As credenciais do portador do cartão seriam validar pelo sistema de atendimento a fim de garantir a identidade do portador do cartão. O sistema de atendimento pode credenciar cada prestador junto ao conselho estadual de examinadores médicos a cada ano e o cartão de prestador pode facilitar as renovações anuais.

Os cartões dos prestadores podem ser usados a fim de acessar Sistemas de Informações Clínicas (CIS) diferentes se estão conectados a uma rede privada comum (como uma VPN) e possuem a permissão por meio de senha do paciente. Por exemplo, se o Sr. Stewart, um paciente do Dr. Jones na Universidade de Washington adoece enquanto está viajando para Nova York, o Dr. Peck em Cornell pode ter acesso ao registro eletrônico proveniente de Seattle do Sr. Stewart através da inserção do cartão do paciente 132 e a digitação da senha. Se Cornell e U.W. são assinantes da Rede Privada GPMR, o Dr. Peck pode, portanto, ler o registro armazenado em um Cerner-CIS (um primeiro sistema proprietá rio) em Seattle, mesmo que use regularmente um HBOC-CIS (um

segundo sistema proprietário) em Cornell. Isso proporciona uma conectividade funcional, porém não fornece uma interoperabilidade campo-a-campo verdadeira. Elimina-se a necessidade de padrões de interoperabilidade e permite-se diferentes sistemas de modo que possam se comunicar entre si com eficiente através somente do acesso de segurança de compartilhamento. Protege-se os sistemas CIS proprietár ios, à medida que é promovido o acesso universal.

O servidor 120 fornece um Sistema Operacional Clínico (COS) que pode conectar diversas estações a um registro integrado comum que opera em tempo real. O COS forneceria a interoperabilidade campo-a-campo verdadeira já que a estrutura de campo seria a mesma para cada sistema de atendimento que a usa. O sistema COS pode criar um processo para um "regist ro longitudinal" em que cada ocorrência original de cuidados médicos é anexada com o decorrer do tempo e por meio dos sistemas de atendimento em um único registro médico. Em um sistema de registro longitudinal, a "reconstrução" não é necessária. Cuidados médicos intercalados são evitados e a continuidade é encorajada, visto que os erros sistemático s podem ser amplamente evitados. Por exemplo, a quinta maior causa de mortes nos Estados Unidos da América são as interações medicamentosas adversas, as quais podem ser amplamente evitadas através da conexão de todos os indivíduos em questão ao mesmo sistema farmacêutico e através da operação do sistema em tempo real.

O software integrado COS pode automaticamente coletar dados a partir dos processos usuais de cuidados médicos e pode lançar automaticamente os dados coletados em uma base de dados relacional a fim de analisar os resultados das variações naturais nos cuidados médicos entre os praticantes. A base de conhecimento gerada a partir da coleta dessa variação pode ser usada de modo a otimizar os cuidados médicos para populações inteiras. A aná lise do resultado pode ser usada para criar protocolos baseados em indício s para, então, diminuir a variação na padronização dos cuidados médicos para os melhores resultados. Esse processo pode reduzir os erros médicos, otimizar os resultados de cuidados com a saúde, salvar vidas e diminuir substancialmente o custo de tais cuidados.

Em operação, o sistema 100, em diversas modalidades, permite o acesso autorizado aos registros médicos armazenados por meio do servidor 120. Quando um

cartão de prestador é inserido em uma estação 104 e autenticado (108), uma chave de sessão é gerada (110) pelo cartão e enviada ao servidor 120 juntamente com o nome do portador do cartão, o número de Identificação e o nível de acesso. O servidor inicializa uma nova sessão (134) e armazena (122 e 124) essa informação para uso futuro. Essa informação da sessão é retida mesmo após o cartão do prestador ter sido removido (106). Dependendo da aplicação, quando o cartão do prestador é removido, a aplicação irá retornar à página de início da sessão ou exibir um aviso para Inserir o Cartão do Paciente. A sessão se mantém ativa até (a 140): o usuário se desconecta da estação 136, o período de tempo de espera do cartão de 15 (por exemplo) minutos expira (112); o período de tempo de espera da sessão do servidor (138) expira; ou o usuário fecha a janela do navegador.

Após um cartão de prestador 102 ter sido autenticado e removido, um cartão de paciente 132 pode ser inserção em uma estação 136 e lido (130). Um nível de acesso do prestador determina quais informações sobre o cartão do paciente 132 podem ser visualizadas. Se o paciente é um assinante do mesmo grupo do plano de saúde ao qual o prestador pertence, nenhum consentimento adicional (por exemplo) é exigido para que o prestador visualize (142) e modifique (144) informações. Se o prestador não pertence ao mesmo grupo do plano de saúde, pode-se exigir que o paciente entre com sua senha, a qual pode atuar como um consentimento legal para liberar as informações médicas. Para ver as informações que o paciente marcou como confidencial, pode-se exigir que o paciente entre com sua segunda senha a fim de consentir o acesso àquelas informações.

Quando o cartão do paciente 132 é removido, o registro do paciente é encerrado, a aplicação retorna à página de entrada no sistema e, previamente, as páginas visualizadas são removidas do cachê. A sessão original pode se manter ativo e um cartão de um paciente diferente pode ser inserido e visualizado sem uma nova autenticação do cartão do prestador.

Embora a invenção tenha sido aqui descrita por meio de modalidade exemplificativas, as variações nas estruturas e método ora descritos podem ocorrer sem que se desvie do espírito e do escopo da invenção. Por exemplo, o posição e/ou dimensionamento de diversos componentes podem variar. Os componentes e disposições

individuais dos componentes podem ser substituídos conforme conhecido na técnica (PDAs, telefones celulares, cartões de memória, chips incorporados de radiofreqüência e similares). Visto que muitas modalidades da invenção podem ser realizadas sem que se desvie do espírito e escopo da invenção, a invenção não é limitada, exceto pelas reivindicações em anexo.

## REIVINDICAÇÕES

1. Sistema de segurança para registros médicos **CARACTERIZADO** pelo fato de que compreende: Um mecanismo de segurança configurado para autenticar um dispositivo de mídia legível por computador do consumidor que compreende um primeiro mecanismo de autenticação e uma memória para o armazenamento das informações do consumidor que compreende informações provenientes de um histórico do consumidor, e para autenticar um dispositivo de mídia legível por computador do provedor que compreende um segundo mecanismo de autenticação; um armazenamento de dados para armazenar o histórico do consumidor; e um servidor que, em resposta à autenticação bem sucedida dos dispositivos de mídia legível por computador do consumidor e do provedor, concede ao provedor o acesso às informações armazenadas na mídia legível por computador do consumidor e/ou concede o acesso ao histórico do consumidor no armazenamento de dados.

2. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o primeiro e segundo mecanismos de autenticação compreendem chaves emitidas pelo mecanismo de segurança.

3. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o servidor transfere dados do armazenamento de dados para o dispositivo de mídia legível por comp utador do consumidor.

4. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o servidor armazena uma ocorrência de cuidados médicos no histórico do consumidor quando uma ocorrência de cuidados médicos é fornecida ao consumidor.

5. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dispositivo de mídia legível por computador do consumidor possui nível de segurança para conceder diferentes níveis de ac esso às informações do c onsumidor.

6. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mídia legí vel por computador do consumidor armazena um localizador para acessar o servidor através de uma rede.

7. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mídia legível por computador do provedor armazena informações do

provedor sobre a licença médica.

8. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mídia legível por computador do consumidor compreende uma senha para permitir o acesso direto às informações do consumidor.

9. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dispositivo de mídia legível por computador do consumidor compreende informações para autorizar o pagamento de serviços prestados ao consumidor.

10. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dispositivo de mídia legível por computador do provedor compreende informações sobre o seguro para efetuar a cobrança a terceiros dos serviços prestados para o consumidor pelo provedor.

11. Aparelho, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mídia legí vel por computador do consumidor compreende um identificador biométrico para permitir o acesso direto às infor mações do consumidor.

12. Método para acesso seguro dos registros médicos **CARACTERIZADO** pelo fato de que compreende: autenticar um cartão do provedor e estabelecer uma sessão segura com um servidor; autenticar um primeiro cartão do consumidor que armazena informações do consumidor que compreendem ocorrências do histórico de consumidor sobre um consumidor; acessar um armazenamento de dados que armazena o histórico do consumidor somente quando a sessão segura está ativa; e fornecer informações acessadas para um terminal que é associado ao cartão autenticado do provedor.

13. Método, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende, adicionalmente, o encerramento da sessão segura e o esvaziamento de caches associados ao histórico do consumidor.

14. Método, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende, adicionalmente, a autenticação de um segundo cartão do consumidor quando a sessão segura ainda está ativa.

15. Método, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que o armazenamento de dados é acessado com o uso de senhas para diferenciar níveis de segurança que estão associados ao cartão do consumidor.

16. Método, de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que o armazenamento de dados pode ser acessado sem o uso de uma das senhas quando o cartão do consumidor e o cartão do provedor são associados à mesma entidade do seguro.

17. Método, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende, adicionalmente, editar o conteúdo do cartão de consumidor em resposta aos dados acessados.

18. Sistema para acesso seguro dos registros médicos **CARACTERIZADO** pelo fato de que compreende: Meios para a autenticação de um cartão do provedor e o estabelecimento de uma sessão segura com um servidor; meios para a autenticação de um primeiro cartão do consumidor que armazena informações do consumidor que compreendem ocorrências do histórico de consumidor sobre um consumidor; meios para o acesso de um armazenamento de dados que armazena o histórico do consumidor apenas quando a sessão segura está ativa; e meios para o fornecimento das informações acessadas para um terminal associado ao cartão autenticado do provedor.

19. Método, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de compreender, adicionalmente, meios para a finalização da sessão, mediante o término de um processo de limite de tempo.

20. Método, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende, adicionalmente, a autenticação de um segundo cartão do consumidor quando a sessão segura ainda está ativa.

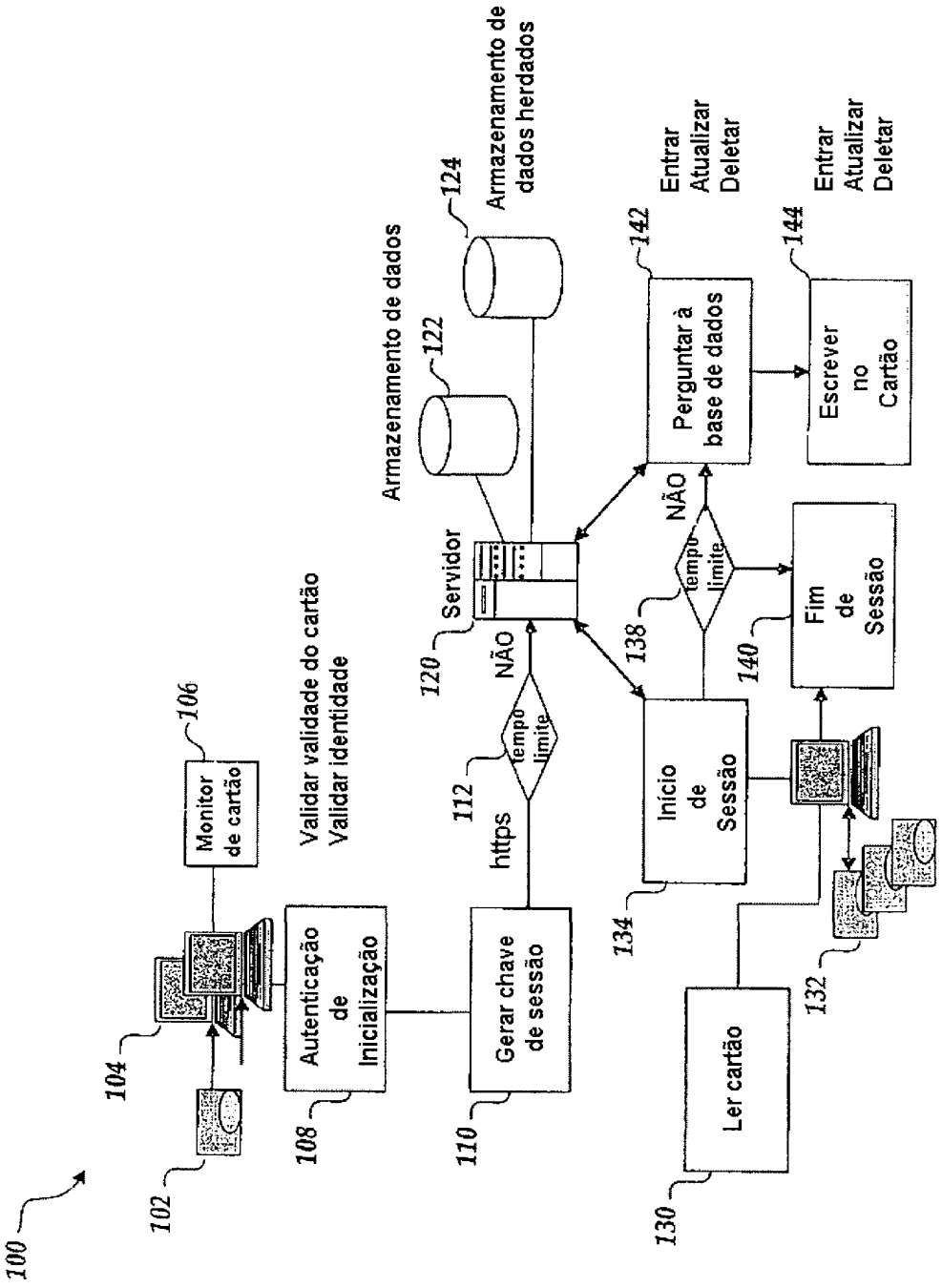

100
102
104
106
Monitor de cartão
Validar validade do cartão
Validar identidade
Autenticação de Inicialização
108
Gerar chave de sessão
110
https
112
tempo limite
NÃO
120
Servidor
Armazenamento de dados
122
Armazenamento de dados herdados
124
138
tempo limite
NÃO
Perguntar à base de dados
142
Entrar
Atualizar
Deletar
Escrever no Cartão
144
Entrar
Atualizar
Deletar
Início de Sessão
134
Fim de Sessão
140
132
Ler cartão
130

*Fig. 1*

## RESUMO

**"SISTEMA DE SEGURANÇA PARA REGISTROS MÉDICOS; MÉTODO PARA ACESSO SEGURO DOS REGISTROS MÉDICOS; E SISTEMA PARA ACESSO SEGURO DOS REGISTROS MÉDICOS".**

Trata-se de um sistema seguro para acessar os registros que utiliza um dispositivo de mídia do provedor e um dispositivo de mídia do consumidor para acessar os registros associados ao consumidor. Ambos os dispositivo de mídia do consumidor e do provedor são autenticados automaticamente antes que o acesso aos registros do consumidor seja concedido. Os registros podem ser armazenados centralizadamente em um local central e transferido por download, por completo ou parcialmente, ao dispositivo de mídia do consumidor. As senhas podem ser usadas a fim de conceder acesso local ao dispositivo de mídia do consumidor, por exemplo, na ausência de conectividade da rede.