46b173b0f82ebc72dbd3dced710b30e469de.pdf

Security and Privacy Issues with Health Care Information Technology

analisamos o movimento para os registros eletrônicos de pacientes (EPR) e o uso de redes de sensores para o monitoramento remoto do paciente.

Com as organizações de cuidados de saúde que se deslocam para EPRs, as informações que já foram armazenadas em formato de papel serão agora armazenadas eletronicamente permitindo fácil acesso e uso. Apoiando essa transição, a IEEE uniu forças com a Associação Médica Americana e outras oito importantes sociedades de medicina e engenharia não lucrativas para formar um consórcio de guarda-chuva, o ***Conselho de Biotecnologia*** [1].

O objetivo principal do conselho é padronizar tudo, desde terminologia médica até protocolos de rede para que os registros médicos possam ser armazenados eletronicamente e serem enviados de imediato para qualquer lugar do mundo.

Tanto a indústria como as instituições acadêmicas estão desenvolvendo sistemas de sensores para o monitoramento remoto de pacientes. Por exemplo, o Integrated Digital Hospital (IDH) da Intel tem como objetivo melhorar os cuidados de saúde em todo o mundo, ligando pessoas, processos e tecnologias [17]. O sistema IDH combina o ponto de atendimento móvel (MPOC) e outra tecnologia da informação para integrar a informação paciente e administrativa em uma visão abrangente e digital da saúde do paciente. O projeto de tecnologia da informação para o trabalho assistido em casa (ITALH) na Universidade da Califórnia, Berkeley, está a analisar as redes de sensores para o monitoramento remoto dos pacientes [6]. Este projeto visa criar um sistema baseado em sensores portáteis que permitirão às pessoas que necessitam de assistência para viver em casa para fazê-lo usando tecnologia da informação. A Universidade Estadual do Kansas e a Universidade do Alabama em Huntsville têm um esforço combinado trabalhando em Infraestruturas de Redes Corporais de Área Larga (WABN) [12]. Eles estão desenvolvendo sistemas de monitoramento de estado de saúde wearable que podem ser usados ​​para o monitoramento do paciente.

Essas tecnologias fornecerão muitos benefícios para a prestação de cuidados de saúde, mas há uma série de implicações de segurança e privacidade que devem ser exploradas para promover e manter os princípios éticos e sociais fundamentais. Essas questões incluem direitos de acesso aos dados, como e quando os dados são armazenados, segurança da transferência de dados, direitos de análise de dados e políticas governamentais. Embora existam regulamentos atuais para dados médicos, estes devem ser reavaliados como uma adaptação de novas tecnologias que alteram a forma como a assistência médica é feita.

Médicos, enfermeiros, companhias de seguros e pacientes podem acessar todos os registros pela Internet. EPRs reduzem o número de erros devido à ilegibilidade e inconsistência de termos. Além disso, os registros eletrônicos podem ser copiados com mais facilidade do que os registros em papel que impedem a perda de dados [10], [1].

A implementação de EPRs inclui uma base de dados local que coleta toda a informação para registros de pacientes em um determinado local. Por exemplo, cada hospital pode ter seu próprio banco de dados eletrônico de informações do paciente. Essas bases de dados locais podem então ser conectadas via Internet para transmissão de dados, de modo que um médico em um hospital possa visualizar as informações de um paciente de outro hospital.

Diferentes tipos de sensores podem ser usados em casa para monitorar os sinais vitais de um paciente. Dispositivos portáteis, como sensores de eletrocardiograma e oxímetros de pulso, estão sendo usados juntamente com sensores de temperatura e umidade ambiente não usuais. Novos sensores também estão sendo desenvolvidos para fazer diferentes formas de monitoramento. Por exemplo, detectores de queda portáteis que incluem acelerômetros estão sendo desenvolvidos pela ITALH [2].

Na maioria desses sistemas, um relatório periódico dos sensores é enviado de volta via comunicação sem fio, usando ZigBee, Bluetooth ou outras tecnologias, para uma estação base local dentro da casa. Esta estação base local, e. um computador pessoal, avalia os dados enviados pelos sensores. Por exemplo, se os dados de uma anormalidade nos sinais vitais aparecem, a estação base local pode enviar os dados do sensor, juntamente com um alarme, para uma estação central de monitoramento. Isso permite que os prestadores de cuidados de saúde na estação central de monitoramento tomem as medidas apropriadas para ajudar o paciente. A transmissão das informações entre o lar e o site de monitoramento é feita através da Internet. Este tipo de sistema restringe minimamente as atividades diárias dos pacientes, enquanto ainda permite que ele / ela seja monitorado.

Para obter o máximo benefício dessas tecnologias, os dois sistemas podem ser integrados. Uma vez que os dados do sensor são transmitidos para a estação central de monitoramento, ele pode ser incorporado no EPR do paciente. Esta informação pode ser usada para ajudar a melhorar a prestação de cuidados de saúde, fornecendo uma descrição mais detalhada da situação médica do paciente.

Embora as tecnologias acima mencionadas possam ajudar a melhorar a qualidade geral da prestação de cuidados de saúde, os benefícios dessas tecnologias devem ser equilibrados com as preocupações de privacidade e segurança do usuário. Os dados de sensores internos e registros médicos serão comunicados eletronicamente via internet e transmissões sem fio. Isso aumenta o perigo de comprometer a segurança e a privacidade dos indivíduos

A conexão de informações de saúde pessoal à Internet expõe esses dados a ataques mais hostis em comparação aos registros médicos baseados em papel.

No entanto, uma vez que esta informação está disponível eletronicamente, abre a porta para hackers e outros atacantes mal-intencionados para acessar os registros, bem como aqueles que estão autorizados. Além disso, dada a natureza distribuída das redes de sensores para o monitoramento do paciente interno, há um maior desafio para garantir a segurança e integridade dos dados em comparação com o sistema tradicional de cuidados de saúde.

* Quem possui os dados? Quem tem autoridade para excluir, editar e adicionar informações aos dados de saúde, bem como aplicar os regulamentos em torno dele? Os pacientes individuais possuem dados coletados em si mesmos? Os seus médicos possuem os dados? Os seus provedores de seguros possuem os dados? São todos os co-proprietários? A questão de "quem é o dono dos dados" é particularmente problemática e inesgotável. Foi objeto de processos recorrentes e altamente divulgados e de inquéritos ao Congresso. Além disso, algumas HMOs se recusaram a cobrir as despesas de um paciente quando o paciente participou de protocolos de tratamento clínico que são experimentais [3]. Isso traz a questão de que, se o provedor de seguros não possuir os dados do paciente, eles podem se recusar a pagar as despesas associadas à coleta e armazenamento dos dados? Esta questão, por sua vez, afeta os direitos de terceiros. Se os dados são passados ​​para um terceiro, eles têm a mesma autoridade que o proprietário dos dados, ou seus direitos são mais estreitos? Não está claro qual o nível de privacidade e proteção de segurança que deve ser mantido quando os dados são transferidos para um terceiro.
* Que tipo de dados e quantos dados devem ser armazenados? Notas de médicos, ressonâncias magnéticas e resultados de testes de laboratório são exemplos de dados armazenados no registro de papel do paciente. Em relação aos EPR, todos esses dados devem ser armazenados eletronicamente ou um subconjunto desses dados será suficiente para fins de cuidados de saúde? Por exemplo, os dados podem ser agregados e os resultados armazenados, e isso pode ser informações suficientes para os usuários do EPR. Esta questão também se aplica ao caso de monitoramento remoto de pacientes usando redes de sensores. Por exemplo, a maior parte dos dados brutos deve ser armazenada localmente na residência do paciente, enquanto apenas os dados agregados necessários para o diagnóstico e a resposta de emergência são transmitidos de volta ao centro de monitoramento? A quantidade de dados do sensor que está armazenada na localização central precisa ser suficiente para realizar as tarefas relacionadas ao atendimento ao paciente. Qualquer informação extra não terá um impacto significativo no atendimento ao paciente, mas pode comprometer ainda mais a privacidade do indivíduo. Em ambos os casos, a granularidade dos dados coletados e armazenados precisa ser minimizada, tanto quanto possível, enquanto ainda atinge o nível desejado de cuidados de saúde.
* Onde os dados de saúde devem ser armazenados? Esta é uma questão de armazenamento centralizado versus descentralizado. No caso dos EPRs, os dados devem residir em bancos de dados locais que podem ser conectados uns aos outros ou devem ser armazenados em um banco de dados central? No caso do monitoramento remoto do paciente, os dados do sensor bruto devem ser armazenados apenas localmente ou devem ser armazenados na estação central de monitoramento? Que tipo de armazenamento de dados irá melhor acomodar as necessidades de privacidade e segurança?
* Quem pode visualizar o registro médico de um paciente? Nós dividimos os usuários de EPR em duas categorias: a) usuários com privilégios de leitura / gravação - como médicos e enfermeiros, que não só podem visualizar o EPR de um paciente, mas também editar os registros. b) usuários com privilégios de somente leitura, por exemplo, o provedor de seguros pode limitar-se apenas a visualizar o EPR do paciente, mas não pode editá-lo. Dependendo do usuário que acessa o EPR, pode haver restrições adicionais sobre quais partes dos dados aos quais seus privilégios se aplicam. Por exemplo, no caso de um provedor de seguros, seu acesso pode ser limitado à parte do EPR que facilita o reembolso de despesas médicas. Em outro exemplo, um paciente idoso pode querer autorizar a visualização parcial de seu registro médico para certos parentes.
* Para quem esta informação deve ser divulgada sem o consentimento do paciente? Existem situações nas quais a informação de saúde do paciente precisa ser divulgada a outras pessoas além dos usuários previamente autorizados. Por exemplo, no caso de monitoramento remoto do paciente, uma emergência pode exigir a divulgação de dados de saúde sem o consentimento do paciente para que esse paciente receba os cuidados necessários.

Embora o tipo de mineração de dados feito nesta informação tenha preocupações de segurança e privacidade, a heterogeneidade dos bancos de dados e a dispersão dos dados em todas as instalações de cuidados médicos sem qualquer formato comum ou princípios de organização, restringem o que pode ser feito. À medida que as EPRs se generalizam, mais organizações de saúde terão bancos de dados que armazenam a informação do paciente em um formato informatizado comum. Estes dados podem então ser facilmente compartilhados através da rede de comunicação, o que criará uma fonte maior de dados médicos humanos. Dado esse aumento nos dados disponíveis, o papel da mineração de dados e de como é governado precisa ser avaliado.

A partir da mineração em dados médicos, pode-se categorizar e pesquisar pacientes com base em inúmeros fatores como idade, gênero ou doença. Isso pode levar a efeitos discriminatórios e de exclusão. Como esses dados se tornam mais uma "mercadoria" que pode ser transmitida pela Internet e coletada, é importante que o anonimato dos dados ocorra antes de qualquer mineração de dados ter lugar. A questão do que implica o anonimato e os regulamentos para divulgação de dados aos usuários, como avaliadores de cuidados gerenciados e companhias de seguros, devem ser respondidas em termos de mineração de dados.

Os dados anônimos podem ocorrer em vários níveis. Por exemplo, remover identificadores pessoais, como nome, idade e número de segurança social, podem dificultar a ligação de dados a um indivíduo único. No entanto, mesmo isso pode não fazer com que o dado seja bastante útil para evitar os efeitos discriminatórios. Os dados, embora não correlacionados com um indivíduo único, podem ser vinculados a uma subpopulação maior, como pessoas que pertencem à região específica da população ou pessoas do gênero / raça. O que o nível adequado de anonimato é para uma determinada tarefa de mineração de dados deve, portanto, ser avaliado.

Isso leva à questão de quem deve ter acesso aos dados e a que nível de anonimato. As informações de um PC para monitoramento do paciente em casa podem enviar os dados para o hospital com alguma marca de identificação para sinalizar de que paciente os dados estão vindo. O médico precisa saber quem é o paciente e pode precisar fazer alguma mineração nos dados ao longo do tempo, mas o provedor de seguros? Qual o nível de conhecimento que os provedores diferentes obtêm? Qual o nível de capacidade de mineração de dados, se diferentes provedores puderem ser permitidos? As práticas éticas não são bem definidas para a vasta gama de divulgações para usuários secundários, como avaliadores de cuidados gerenciados e companhias de seguros1. Estas questões relacionadas com a mineração de dados precisam ser avaliadas e os regulamentos implementados para maximizar os benefícios de ter mais dados médicos disponíveis, minimizando os efeitos nocivos.

Atualmente, existem muitos regulamentos e regras diferentes em torno de cuidados de saúde, incluindo os regulamentos federais da Lei Americana de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA), bem como vários regulamentos estaduais.

O objetivo da HIPAA é garantir que todos os registros médicos, cobranças médicas e contas de pacientes atendam a certos padrões consistentes em relação à documentação, manejo e privacidade. Além disso, HIPAA exige que todos os pacientes possam acessar seus próprios registros médicos, corrigir erros ou omissões e estar informado sobre como as informações pessoais são compartilhadas ou usadas.

ada estado tem regras especializadas sobre como os cuidados de saúde são tratados, que são bem descritos pelo Estado de Saúde da Saúde, do Projeto de Privacidade [13].

Por exemplo, o Código do Alabama não tem um estatuto geral que concede aos pacientes o direito de acessar seus próprios registros médicos. Também não possui um estatuto geral que restrinja a divulgação de informações confidenciais. No entanto, em relação a certas condições médicas, como distúrbios de saúde mental e doenças sexualmente transmissíveis, o Alabama possui alguns estatutos que controlam o acesso de um paciente à informação e a divulgação desta informação.

Em contraste, os estatutos da Califórnia concedem aos pacientes o direito de acesso à sua informação de cuidados de saúde de prestadores de cuidados de saúde, HMOs, seguradoras e agências estatais. O Código da Califórnia também possui regulamentos extensivos sobre divulgação e uso de informações de cuidados de saúde por essas entidades.

Existe a necessidade de ter políticas coesas para proteger a informação de saúde pessoal sensível à medida que se torna disponível eletronicamente. Com os códigos de estado variáveis, há incertezas na propriedade de dados, direitos de acesso e divulgação, pois os dados podem ser transmitidos por linhas estatais eletronicamente. Os mandatos HIPAA de proteção à privacidade de 2003 são uma base para um padrão nacional para a privacidade em saúde [14].

As questões de acesso, armazenamento e análise de dados não são únicas na arena médica. Esses problemas foram analisados em várias áreas, desde serviços financeiros até compras na internet, e existem soluções técnicas que podem ser aplicadas aos cuidados de saúde para aumentar a privacidade e segurança em uma configuração multiusuário:

Desenvolvimento de políticas: é necessário criar novas políticas que possam lidar com toda a jurisdição estadual. Enquanto as Regras de Privacidade HIPAA fornecem algumas bases, é necessário fazer mais para criar regras claras sobre as quais os usuários possam confiar. O movimento em direção a EPRs e a crescente quantidade de dados médicos que serão reunidos devido a redes de sensores remotos, possibilitam a transferência de grandes quantidades de dados rapidamente. Isso requer um conjunto compreensivo de regulamentos que protejam a privacidade e a segurança do usuário, independentemente do estado em que os dados estão localizados.