INTRODUÇÃO:

O problema mais recente envolve a preocupação com confidencialidade no ambiente das instituições de saúde.

Questões:

Quem possui os dados no registro de saúde pessoal da Sra. Powter?

Quando a Sra. Powter sai do Plano de Saúde nº 1, o que acontece com os dados dela?

Quais são os problemas (por exemplo, padrões de intercâmbio de dados, custo) que ocorrem ao transferir dados entre os planos de saúde?

Que outras utilizações secundárias dos dados devem ser permitidas?

Se a Sra. Powter receber permissão para cada instância de uso ou deveria dar permissão global?

ao dar consentimento, até que ponto os hospitais se certificam que têm medidas de segurança para tratar os meus dados?

O que fazem ao dispositivo em fim de vida?

Entregam a um determinado laboratório para investigação?

Dentro do hospital ou não?

Quais são os potenciais benefícios e riscos em relação ao uso secundário de dados de saúde?

• Quem possui dados de saúde e quem tem o direito de acessar os dados e para que fins?

• Quais são os problemas de confiança pública em evolução em relação ao consentimento do paciente para o uso secundário de dados de saúde? Os pacientes têm o direito de auditar ou colocar outras restrições sobre o uso de seus dados, mesmo após a anonimização?

• À luz de graves ameaças à saúde pública, como a gripe aviária, como a sociedade concilia o bem público com os direitos dos indivíduos enquanto pesa considerações de saúde versus privacidade?

• Quais os problemas que podem surgir à medida que as tecnologias inovadoras melhoram a capacidade e a facilidade do compartilhamento generalizado de dados e de usos comerciais adicionais?

• O que pode ser feito para abordar questões decorrentes de uso inapropriado e / ou exploração de compartilhamento de dados?

• Que regulamentos, legislação e / ou políticas e procedimentos são necessários para abordar essas questões?

O sector da saúde é caraterizado pelas seguintes tendências:

* Dados e informação sobre doentes é recolhida através de uma vasta quantidade de sistemas de TIC e de equipamentos médicos. Frequentemente, não existe ou existe pouco conhecimento sobre o armazenamento dos dados dos pacientes.
* O tratamento moderno de doentes está fortemente dependente de dados e de informação, como a medicina de precisão ou as vias de cuidados pessoais.
* Dados e informação são partilhados para outros objetivos que não o tratamento direto dos mesmos. Tal poderá ser para investigação, gestão de saúde pública ou gestão da procura através dos sectores.
* Dados e informação são utilizados conjuntamente com analítica, Big Data e sistemas cognitivos para permitir novos regimes de tratamento e novos modelos de negócio.

Para além dos muitos benefícios associados ao surgimento e evolução destas tecnologias, estas permitiram que surgissem novas ameaças à segurança da informação. É então, cada vez mais necessário, o desenvolvimento, implementação e utilização de mecanismos de segurança, que possam proporcionar os serviços básicos de segurança (e.g. autenticação, controlo de acesso, confidencialidade, integridade e não-repúdio).

Nos cuidados de saúde devem ser considerados 2**níveis de prestação de cuidados**que têm necessidades diversas (<http://im.med.up.pt/epr/epr.html>):

* **Cuidados primários** - onde os sistemas de informação podem ser utilizados para a prestação de cuidados directamente ao paciente e de uma forma global, com partilha de informação clínica com os cuidados hospitalares, facilitando cuidados partilhados.
* **Cuidados hospitalares**- neste caso concreto quando se fala de sistemas de informação hospitalares, estes estão adaptados às múltiplas especialidades, tendo estas necessidades distintas, que são reflectidas nos sistemas de informação que utilizam.   
  Exemplos: aplicações para áreas clínicas, laboratoriais ou radiológicas.

Podemos separar o problema da segurança em dois, o que tem a ver com as vulnerabilidades dos sistemas de informação e o que tem a ver com os problemas com as pessoas, mas precisamente com os profissionais que tem acesso as dados.

A cibersegurança será o principal desafio para as instituições hospitalares uma vez que o número de ameaças bem-sucedidas nestas instituições cresceu significativamente nos últimos meses. Sabe-se que, nos Estados Unidos, mais de 110 milhões de registos individuais de saúde foram alvo de ciber-ataques em instituições hospitalares; facto que representa um número 3 vezes superior de indivíduos afetados quando comparado com o total de ameaças ocorridas entre 2009 e 2014. (<http://spms.min-saude.pt/seguranca-da-informacao/>).

Um em cada três consumidores encontram-se em risco de ter os seus registos de saúde violados, sendo  crescentemente expostos ao roubo da sua identidade financeira  e ao roubo de identidade médica. Segundo um estudo da *Medical Identity Theft Alliance* (MIFA), o roubo de identidades médicas cresceu cerca de 22%, podendo este número ser superior.

As pesquisas atuais sobre proteção da privacidade do paciente em sistemas de informações de saúde são centralizadas em torno da proteção do EHR - isto é, para proteger a informação do paciente de serem abusados ​​por usuários autorizados ou ser acessados ​​por pessoas fora de uso não autorizadas ou ser re-identificados a partir de dados de saúde publicados para uso secundário .

Existem quatro formas de identificação de dados do paciente (d43f81c6e8c3e46f5bdcb686d60d40915de8.pdf):

* Os dados anônimos são dados que foram coletados para que a identificação do paciente fosse removida no momento em que a informação foi coletada. Os identificadores do paciente não são registrados no momento da coleta da amostra e, portanto, nunca podem ser recuperados.
* Os dados anônimos são dados que são coletados inicialmente com os identificadores do paciente, que posteriormente são removidos irrevogavelmente. Ou seja, nunca pode haver possibilidade de retornar ao registro do paciente e obter informações adicionais.

dados anônimos, como descrito acima, podem ser duplicados acidentalmente e não podem ser verificados para correções ou dados adicionais.

* Dados des-identificados são dados coletados inicialmente com os identificadores do paciente, que posteriormente são codificados ou criptografados. O paciente pode ser re-identificado nas condições estipuladas por uma agência apropriada, tipicamente um Conselho de Revisão Institucional (IRB).
* Os dados identificados só podem ser coletados sob revisão significativa pela instituição, diretrizes federais, etc., com o paciente dando consentimento informado por escrito.

Os usos secundários dos dados de saúde podem melhorar as experiências de cuidados de saúde dos indivíduos, ampliar o conhecimento sobre doenças e tratamentos, fortalecer a compreensão da eficácia e eficiência dos sistemas de cuidados de saúde, apoiar a saúde pública e os objetivos de segurança e ajudar as empresas a atender às necessidades dos clientes.

No entanto, o acesso e o uso de dados de saúde representam desafios éticos, políticos, técnicos e econômicos complexos.

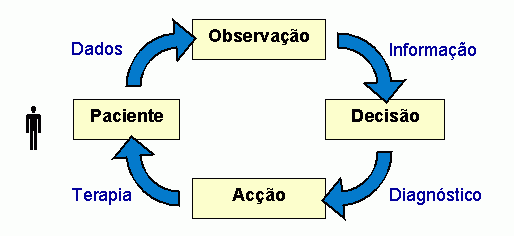
Por exemplo, para atender aos requisitos de saúde pública, preparação para emergências e segurança interna, o governo federal iniciou a coleta de dados em tempo real de salas de emergência e outras fontes - sem diálogo público, com base na autoridade da legislação vigente em saúde pública. Além disso, há relatos de compra e venda de dados não anônimos de pacientes e provedores pela indústria médica - realizados sem o consentimento explícito de pacientes ou médicos. (367969507b2209c94a4b23992a50d425dfab.pdf)

DESENVOLVIMENTO:

A recolha da informação médica é feita durante uma consulta médica, essencialmente através da narrativa do doente, de exames complementares e, eventualmente, através da consulta ao processo e à ficha clínica anterior do doente.

A informação existente num processo clínico corresponde a informação maioritariamente alfanumérica, ou seja, que pode ser representada por **carateres**ou **dígitos**. A restante informação, fundamentalmente aquela proveniente dos meios complementares de diagnóstico, como **sinal** ou **imagem**, habitualmente não está disponível juntamente com o processo clínico (ex: imagens das endoscopias só são visualizadas quando explicitamente solicitadas), não ficando toda a informação clínica de um dado doente disponível como um todo.

Na realidade muitas das vezes os profissionais não dispõem da informação completa sobre os doentes, o que poderá refletir-se na qualidade e nos resultados da sua intervenção. Estas falhas de comunicação podem conduzir a quebras na continuidade dos serviços prestados, a tratamentos/procedimentos inadequados ou pouco eficazes, com efeitos negativos para o bem-estar do doente (Comunicação em saúde e a segurança do doente: problemas e desafios – revista portuguesa de saúde pública).

 (<http://im.med.up.pt/epr/epr.html>)

O processo clínico em papel é uma forma de registo clínico onde os dados são introduzidos de forma manuscrita, e toda a informação clínica é anexada a este. Este é um sistema de armazenamento, que serve de base à prestação de cuidados de saúde. Assim, necessita de integrar informação proveniente de diversas fontes (<http://im.med.up.pt/epr/epr.html>). Mas com o decorre dos anos este formato em papel começou a desencadear vários inconvenientes devido a:

* Diversidade da estruturação da informação, que depende do médico ou da instituição, ou a falta dela;
* Acesso limitado à informação, devido à organização de forma cronológica;
* Dificuldades no acesso a determinada informação;
* Ilegibilidade dos registos médicos;
* Perdas de informação;
* Duplicação de informação.

E com o avanço da tecnologia, surgiram os processos clínico eletrónicos que visam não só colmatar as limitações referidas, bem como fornecer uma variedade de ferramentas auxiliares que permitem ajudar na decisão clínica, avaliar a qualidade dos cuidados prestados, ajudar na investigação e na educação médica, realizar a gestão e o planeamento dos recursos de saúde, e possibilitar a troca de informação clínica entre cuidados primários e hospitalares. Mas, em contrapartida, toda esta informatização implica um elevado nível de proteção e segurança devido à sensibilidade da informação clínica e pessoal contida nos processos clínicos eletrónicos, necessidade de formação específica dos profissionais de saúde e possibilidade de perda de registos se não forem executados os procedimentos corretos ou perante uma simples quebra elétrica ou no sistema.



As preocupações de proteção e segurança derivam do facto de que as diferentes instituições podem partilhar estas informações entre si, confiando mutuamente que a informação irá ser mantida confidencial e será apenas usada apenas para o propósito definido, assim como nas trocas de informação entre profissionais da mesma instituição, e o resultado desta partilha pode não ser o esperado. É de grande preocupação o facto de que estes profissionais podem aceder à informação médica, não só da rede da sua instituição de trabalho como também de outras redes, o que torna difícil a gestão e a auditoria de quem tem, ou teve, acesso e a que informação, e que mecanismos de segurança deve ter o sistema.

Deve-se ter especial atenção a problemas como a confidencialidade, uma vez que a grande acessibilidade aos dados implica uma grande ameaça para a privacidade das pessoas referentes aos dados, devendo-se adotar medidas para prevenir a ocorrência de acessos não autorizados; a integridade, pois erros nos dados e no software podem acontecer, devendo-se adotar medidas de proteção contra a perda ou corrupção dos dados; e a disponibilidade, dado que as instituições de saúde ficam cada vez mais dependentes do funcionamento dos sistemas de informação, devendo-se adotar medidas para que o acesso autorizado a informação confidencial esteja disponível sempre que necessário. Ver tabela seguinte (<http://im.med.up.pt/seguranca/index.html>):

|  |  |  |
| --- | --- | --- |
|  | **Prevenção** | **Detecção/Correcção** |
| **Confidencialidade** |  |  |
|  | -- controlo de acesso -- autenticação -- encriptação | -- auditoria e monitorização |
| **Integridade** |  |  |
|  | -- assinaturas digitais  -- apoio à introdução de dados  -- standards e codificação -- métodos consistência interna | -- assinaturas digitais -- auditoria e monitorização |
| **Disponibilidade** |  |  |
|  | -- redundância de equipamento -- sistemas recuperação automática | -- auditoria e monitorização -- backups (cópias segurança) -- redundância de equipamento |

Para uma eficaz proteção dos dados deve-se aplicar as medidas de segurança tanto a nível dos equipamentos, das pessoas, do software e dos procedimentos. Claro, que garantir uma segurança perfeita é ainda impossível e é um dos problemas mais estudados atualmente, no entanto é possível reduzir os riscos ou restringir possíveis danos devido à má utilização ou ao uso abusivo dos sistemas de informação.

Todas as instituições estão sujeitas a princípios éticos, e como tal as ações dos profissionais de saúde estão sujeitas a esses princípios, o qual se destaca o sigilo médico. Adicionalmente, quando estes princípios se aplicam no âmbito da Informática, destacar-se desde logo o princípio da privacidade e o princípio da segurança, uma vez que todas os utentes têm o direito à privacidade e ao controlo da recolha, do armazenamento, do acesso, do uso e da transmissão da sua informação médica, e os dados recolhidos por determinado profissional de saúde devem ser protegidos contra a perda, corrupção, destruição, acesso, uso e alteração indevida ou não autorizada.

Perante toda esta disponibilidade da informação clínica aos profissionais de saúde, que por um lado é essencial para uma melhor prestação de serviços, por outro lado pode ser em demasia e põe em causa questões muito séries sobre a segurança dos dados. Inclusive, recentemente, o Bastonário da Ordem dos Médicos, Miguel Guimarães, afirmou o seguinte, "Os médicos têm potencialmente acesso a qualquer informação clínica de um doente e nem sei se deviam ter acesso a todas. Mas não são só os médicos que têm acesso, há outros profissionais que também têm", e, em defesa dos médicos, afirma que, "Isto é um problema atual. Mas quem é responsável pela partilha dessa informação de doentes não são os médicos", uma vez que, "Numa questão em que os dados passam a estar disponíveis num local em que potencialmente podem ter vários utilizadores, tenho dúvidas que a responsabilidade dessa partilha deva ser do médico e não do Estado português".

Como os meus dados são usados:

367969507b2209c94a4b23992a50d425dfab.pdf

* uso primário de dados - o uso da PHI pela organização ou entidade que produziu ou adquiriu esses dados no processo de fornecer atendimento direto em tempo real de um indivíduo.
* uso secundário de dados - uso de cuidados não diretos da PHI, incluindo, entre outros, análises, pesquisas, medições de qualidade / segurança, saúde pública, pagamento, certificação ou acreditação de provedores e marketing e outros negócios, incluindo atividades estritamente comerciais.

Tais usos ocorrem em setores públicos e privados para fins de propriedade, pesquisa e monitoramento com uma regulamentação inferior à abrangente.

O uso de dados de pacientes específicos de pessoas para fins diferentes do atendimento direto ao paciente e saúde pública não é bem compreendido e é mal monitorado. Isso suscita inúmeras questões éticas, técnicas, econômicas e processuais.

Tanto a indústria como as instituições acadêmicas estão desenvolvendo sistemas de sensores para o monitoramento remoto de pacientes. (46b173b0f82ebc72dbd3dced710b30e469de.pdf) Projetos que visam criar sistemas baseados em sensores portáteis que permitirão às pessoas que necessitam de assistência para viver em casa para fazê-lo usando tecnologia da informação que se baseiam em **wireless body area networks** (WABN). 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. 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. 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. Dispositivos portáteis, como sensores de eletrocardiograma e oxímetros de pulso, estão sendo usados juntamente com sensores de temperatura e umidade ambiente não usuais. 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. 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.

Problemas de segurança:

Existem quatro tipos de ameaças que podem ser exploradas indevidamente [21] (DiogoSebe\_SistemaInformacaoEmergenciaMedica.pdf):

• Abuso de privilégios: ocorre quando os utilizadores dispõem de mais privilégios, sobre a base de dados, do que realmente necessitam.

• Abuso legitimo de privilégios: este tipo de abusos acontece quando o utilizador tem privilégios de acesso legítimos, mas intencionalmente explora esses privilégios para aceder a informação de forma maliciosa.

• Promoção de privilégios: as vulnerabilidades de software e os erros existentes na base de dadossãoexploradosdemaneiraaelevarosprivilégiosdotransgressorpermitindo-oaceder a informação de níveis superiores de segurança.

• Vulnerabilidades do sistema operativo: o transgressor exploras certas vulnerabilidades do SO de forma a ganhar acesso não-autorizado à base de dados.

Problemas de segurança na informática:

Mais e mais empresas e indivíduos confiam seus dados em serviços em nuvem e terceirizam tarefas computacionais em seus dados para provedores de serviços de terceiros. Isso suscita preocupações sobre a privacidade das informações sensíveis, uma vez que os dados são armazenados em centros de dados externos ou de base. Em particular, no setor da saúde, os registros de pacientes pessoais sensíveis precisam ser confidenciais. Em (0cc8456950acc93553591f4a79b138bbeaf0.pdf) diz-se que a privacidade das informações confidenciais pode ser garantida, se for codificada pelo proprietário dos dados antes de ser carregada para um serviço na nuvem. Dessa forma, apenas o proprietário de dados legítimo pode acessar os dados, descriptando-os usando sua chave privada de descriptografia. Mas a criptografia limita a possibilidade de terceirizar computação nas informações armazenadas externamente, especialmente se o data center não tiver acesso à chave de descriptografia.

A computação em nuvem apresenta alguns problemas de segurança: verificação de integridade de dados remota, recuperação remota de dados e privacidade de dados.

No entanto, à medida que a Web ganha popularidade e toca muitos aspectos de nossa vida diária, ela se torna a maior fonte de informações pessoais. Os adversários possuem armas poderosas e conhecimento rico, que de alguma forma são fornecidos pelas próprias vítimas. é razoável que possamos levantar a questão: "quando um invasor possui uma pequena quantidade de informações (possivelmente imprecisas) de fontes relacionadas à saúde e associe essas informações com informações acessíveis ao público de fontes on-line, a probabilidade de o atacante seja capaz de descobrir a identidade do paciente alvo e quais são os potenciais riscos de privacidade”. [Primeiro, uma grande quantidade de registros públicos foram acessados ​​on-line, incluindo listas telefônicas, registro de eleitores, registros de nascimento / morte, etc. Embora alguns deles apliquem certas restrições para se defender contra abusadores, ainda é relativamente fácil ou barato rastrear / baixar tais registros. Mais recentemente, sites de redes sociais online, como o Facebook e o MySpace, surgiram para atrair com êxito um grande número de usuários, que voluntariamente colocam suas informações pessoais em sites de redes sociais online para compartilhar com pessoas. Em segundo lugar, com a nova sofisticação das técnicas de recuperação de informação e os avanços das técnicas de busca nos motores de busca, torna-se inesperadamente fácil realizar a extração na escala da Web de informações pessoais dos usuários que estão prontamente disponíveis em várias redes sociais online (por exemplo, [12- 16]). Como resultado, adversários maliciosos ou curiosos poderiam facilmente aproveitar essas técnicas para coletar a informação privada dos outros, que está prontamente disponível em registros públicos online ou em várias redes sociais. Ou: Os usuários de ONS geralmente divulgam voluntariamente suas informações pessoais com detalhes surpreendentes. Por exemplo, os usuários do Linked In listam suas experiências educacionais e de trabalho para buscar possíveis oportunidades de carreira e os usuários do MedHelp compartilham detalhes sobre sua vida e experiências médicas que esperam receber sugestões médicas pertinentes de outros. Ao liberar informações relacionadas à privacidade on-line, um mal-entendido fundamental desses proprietários de informações é que é improvável que vincule informações pertencentes ao mesmo indivíduo de diferentes fontes on-line.] Infelizmente, com os avanços das técnicas de busca e recuperação de informações, é possível que um invasor agregue informações pessoais de um usuário direcionado de diferentes fontes on-line, associando atributos desprotegidos, mas identificáveis ​​ou semi-identificáveis ​​(por exemplo, nomes de conta ou endereço de e-mail idênticos de um usuário descuidado). é altamente possível que um invasor agregue informações diversas de fontes múltiplas (possivelmente relacionadas à medicina) e associe os atributos para identificar um paciente direcionado com alta confiança. [Todo o processo inclui três etapas: ataques de atribuição, inferência e agregação. Na atribuição, os atributos identificáveis, semi-identificáveis ​​ou sensíveis são aprendidos / extraídos de várias fontes na web. Em particular, três tipos de recursos on-line são considerados no exemplo: (1) bancos de dados on-line acessíveis ao público: registros de registro de eleitores, listas telefônicas, registros de nascimento e morte, (2) sites de rede social online com atributos identificáveis ​​explícitos (por exemplo, LinkedIn, Facebook , etc.), bem como redes sociais específicas relacionadas à saúde (por exemplo, MedHelp); e (3) motores de busca comerciais, que indexam uma boa parcela da web. Em inferência, mais atributos são descobertos nas atividades e relacionamentos sociais através da aprendizagem estatística ou do raciocínio lógico. Em agregação, os registros recuperados de diferentes fontes que pertencem potencialmente ao mesmo indivíduo estão vinculados sob evidências fortes ou fracas, nas quais evidências fortes incluem identificadores ou quase-identificadores correspondentes e evidências fracas são semelhanças identificadas a partir de uma perspectiva estatística.] (1471-2105-12-S12-S7.pdf)

Os ciber-criminosos estão a tornar-se mais sofisticados nos seus ataques, levando a um aumento de ameaças em número e em alcance no sector da saúde, devido à perceção destas instituições serem um alvo fácil. No passado, as intromissões ocorriam através de ataques massivos de phishing, utilizando, frequentemente para o efeito, mensagens de correio eletrónico amplamente distribuídas com links maliciosos ou com um anexo que introduzia malware na organização. Presentemente, os ataques de phishing são mais específicos e direcionados (spear phishing e whaling), envolvendo a engenharia social para aceder às credenciais. Os ciber-criminosos aperfeiçoaram também o envio de mensagens de correio eletrónico, tornando-as semelhantes às de fontes legítimas ex.: departamento de TIC das instituições hospitalares, instituições financeiras e outras fontes de instituições fidedignas.

(As ameaças de ransomware, que encriptam ficheiros críticos do sistema tornando-os inacessíveis até que um resgate seja pago, constituem uma ameaça considerável às organizações. O impacto do ransomware vai muito para além da extorsão de dinheiro, pois poderão afetar os cuidados de saúde, as operações diárias e a segurança dos doentes. Quando os sistemas vitais são bloqueados, as equipas têm de recorrer a processos manuais e em papel, o que pode criar atrasos no acesso a informação crítica sobre os doentes e, deste modo, causar atrasos na prestação de cuidados de saúde. Em casos extremos, os hospitais afetados por este tipo de ataques transferiram doentes para outros hospitais e cancelaram agendamentos, por não terem acesso aos registos médicos.) No início de 2016, variantes destrutivas de ransomware como o Locky ou o Samas infetaram computadores individuais e de empresas, em estabelecimentos de saúde e hospitais em todo o mundo. O Ransomware é um tipo de software malicioso que infecta um computador mostrando alertas que indicam ao utilizador que os seus sistemas foram bloqueados ou que os seus arquivos foram encriptados e restringe o acesso dos utilizadores até que uma quantia de dinheiro seja paga para o desbloquear. (<http://spms.min-saude.pt/alertas-e-seguranca/>) O Ransomware é frequentemente transmitido através de e-mails phishing que contêm anexos maliciosos ou através de drive-by download (quando um utilizador visita um site infetado e, em seguida, o malware é transferido e instalado sem o conhecimento do mesmo). Pagar o montante solicitado não garante que os arquivos encriptados sejam disponibilizados; apenas garante que os atores maliciosos recebem o dinheiro da vítima e, em alguns casos, as suas informações bancárias. Além disso, desencriptar ficheiros não significa que o malware em si tenha sido removido.

Para que são usados os meus dados médicos:

Imensos volumes de EHRs são publicados todos os anos para uso secundário, como pesquisa médica, saúde pública, administração governamental e outros serviços relacionados à saúde [2].Um EHR típico consiste em um conjunto de atributos de identificador (por exemplo, nome, SSN), atributos de quase-identificador (por exemplo, gênero, código postal) e atributos sensíveis (por exemplo, doenças). (1471-2105-12-S12-S7.pdf)

* Para prestação de cuidados
* Para prevenir epidemias
* Para investigação:

Quando uma grande quantidade de dados de vários pacientes diferentes, relevantes para uma determinada doença (como o câncer) está disponível, a construção de modelos preditivos a partir desses dados usando o aprendizado de máquina pode contribuir substancialmente para a ciência médica e para o bem público (0cc8456950acc93553591f4a79b138bbeaf0.pdf). Tais modelos podem ajudar a identificar os fatores de risco genéticos e ambientais e constituir a base para a análise preditiva. No entanto, as preocupações com a privacidade, mesmo quando os dados são anonimizados, precisam ser ponderadas.

Tudo isto dá origem a Bancos de dados disponíveis publicamente. Permitindo um maior acesso aos dados, criando assim o maior desafio de privacidade. As diferentes técnicas de preservação da privacidade são potencialmente aplicáveis.

Em primeiro lugar, as empresas privadas que desenvolvem e implantam ferramentas para pesquisa genética acumulam dados através de seus negócios. Dependendo dos acordos com os clientes, eles podem estar obrigados a manter a confidencialidade dos dados do paciente quando a computação de terceirização em tais bancos de dados. Em segundo lugar, hospitais ou clínicas também mantêm registros de pacientes, mas são vinculados por regulamentos e acordos de pacientes para lidar com esses dados com confiança.

A crescente adoção de registros de saúde eletrônicos fornece uma fonte rica para a mineração de dados, a fim de identificar padrões e tendências nos dados de cuidados de saúde. Mas isso implica trocas de informações de saúde. Um sistema para suportar a mineração de dados de informações de saúde deve ser um servidor privado acessível a apenas alguns indivíduos autorizados, com suporte apropriado para implementar a auditoria e outros requisitos para a conformidade. (3e18340408a291897c8c6ea7a0f07289fe54.pdf)

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. 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. (46b173b0f82ebc72dbd3dced710b30e469de.pdf)

Para proteger a privacidade dos proprietários de discos, os EHRs precisam ser desidentificados [3-6] ou anonimizados [7-10] antes de serem publicados. No entanto, mesmo com os dados higienizados, os atributos sensíveis que pertencem a um indivíduo podem ser aprendidos com outros atributos não-sensíveis em combinação com conhecimento externo (por exemplo, lista de registro de eleitores, listas telefônicas, etc.). Os riscos de tais ataques de reidentificação foram intensamente estudados, o que mostra que a quantidade e os tipos de conhecimento externo de um invasor desempenham um papel importante no raciocínio sobre privacidade na publicação de dados. não é fácil, senão impossível, que um editor de dados conheça o conhecimento externo que o atacante possui. Portanto, a pesquisa atual sobre a publicação de dados de preservação da privacidade estuda o problema de uma perspectiva teórica, fazendo suposições sobre o conhecimento de fundo do invasor, quantificando o conhecimento externo, independentemente do seu conteúdo e desinfectando os dados para garantir que a quantidade de divulgação esteja abaixo de um limite especificado. Como resultado, essa proteção, por um lado, não leva em conta que uma grande quantidade de conhecimento externo é acessível aos adversários de várias fontes on-line (por exemplo, redes sociais), por outro lado, pode distorcer muito os dados e seus usos secundários. (1471-2105-12-S12-S7.pdf)

Quando a informação se transforma em resíduo (tertulia\_1.pdf):

Questões específicas:

* Tipo de suporte (papel/digital)
  + Suporte papel: Processo Clínico Meios complementares de diagnóstico Documentos administrativos/Faturação;
  + Suporte digital: CD / DVD/Pen PC/Portátil/Tablet/Servidor/smartphone Equipamentos de meios complementares de diagnóstico/tratamentos médicos;
* Obrigação dos responsáveis pela informação: É a instituição de saúde que é responsável, perante a CNPD, pela destruição dos dados pessoais e por garantir que não há acessos indevidos;
* Responsabilidade das empresas que gerem os resíduos: A responsabilidade da instituição de saúde pode ter sido contratualmente transferida para as empresas de hotelaria hospitalar.

Quando os resíduos têm dados pessoais (tertulia\_1.pdf):

* Estabelecimento de regras
* Orientações escritas
* Especial cuidado no contrato de prestação de serviços
* Declaração do responsável atestando que no material não há dados pessoais
* Formação dos trabalhadores

Artigo 43.º do regulamento 707/2016

Destino do processo clínico em caso de transmissão de consultório

1 — Quando o médico cesse a sua atividade profissional, os seus processos clínicos devem ser transmitidos ao médico que lhe suceda, salvaguardada a vontade dos doentes interessados em que a informação relevante seja transmitida a outro médico por si determinado.

2 — Na falta de médico que lhe suceda, deve o facto ser comunicado à Ordem, por quem receber o espólio do consultório ou pelos médicos que tenham conhecimento da situação, a qual determina o destino a dar -lhes.

Uso e interpretação do dados médicos que as vezes podem ser mais analisados e o doente não sabe:

Artigo 40.º do Regulamento\_707\_2016

Processo clínico, ficha clínica e exames complementares

1 — O médico, seja qual for o enquadramento da sua ação profissional, deve registar, de forma clara e detalhada, os resultados que considere relevantes das observações clínicas dos doentes a seu cargo, conservando -os ao abrigo de qualquer indiscrição, de acordo com as normas do segredo médico.

2 — A ficha clínica é o registo dos dados clínicos do doente, das anotações pessoais do médico e tem como finalidade a memória futura e a comunicação entre os profissionais que tratem o doente.

3 — O doente tem direito a conhecer a informação registada no seu processo clínico, a qual lhe é transmitida, se requerida, pelo próprio médico assistente ou, no caso de instituição de saúde, por médico designado pelo doente para este efeito.

4 — Sempre que tenha de facultar informação do processo clínico o médico tem o direito de expurgar as suas anotações pessoais e o dever de não fornecer informações sujeitas a segredo de terceiros e não comunicar circunstâncias que, a serem conhecidas pelo paciente, poriam em perigo a sua vida ou seriam suscetíveis de lhe causar grave dano à saúde, física ou psíquica.

5 — Os exames complementares de diagnóstico e terapêutica são lhe facultados quando este os solicite, aceitando -se no entanto que o material a fornecer seja constituído por cópias correspondentes aos elementos constantes do processo clínico.

Os regulamentos sobre a divulgação de dados são estabelecidos e legislados para enfrentar a ameaça de privação de infração e melhorar a proteção de dados relacionados à saúde.

Segundo o Regulamento de Deontologia Médica n.º 707/2016, de 21 de Julho, “O Código Deontológico da Ordem dos Médicos é um conjunto de normas de comportamento que serve de orientação nos diferentes aspetos das relações humanas que se estabelecem no decurso do exercício profissional da medicina.”. Diante destas normas, está bem explícita a obrigatoriedade do segredo médico, quer singular ou coletivamente, em unidades de saúde públicas, sociais, cooperativas ou privadas, no que diz respeito às informações que constem do processo individual do doente. É ainda dever das unidades de saúde e dos diretores clínicos impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde.

Consoante o Artigo 32.º do regulamento, o dever de segredo médico deixa de ser aplicado apenas e só mediante o consentimento do doente (ou representante legal), e se a revelação não prejudica terceiros com interesse na manutenção do segredo médico; a necessidade de defesa da dignidade, da honra e dos legítimos interesses do médico, do doente ou de terceiros, não podendo ser revelado mais do que o extremamente necessário à defesa, nem sem a prévia autorização do Bastonário; informações que revelem um nascimento ou um óbito; e de doenças de declaração obrigatória.

Segundo o Artigo 36.º, do Regulamento de Deontologia Médica n.º 707/2016, sobre dados médicos ados, todos os ficheiros, bases e bancos de dados, com informações clínicas sujeitas a segredo médico, devem ser equipados com sistemas, e utilizados com procedimentos de segurança, que impeçam a consulta, alteração e destruição de dados por pessoas não autorizadas e que detetem desvios de informação, caso não se verifiquem estas condições, não devem estar conectados com outros tipos de redes informáticas. Os médicos responsáveis por estes dados, bem como os profissionais que tenham conhecimento dos dados pessoais neles contidos, são obrigados ao segredo, mesmo após o termo de funções.

NOVO REGULAMENTO DA PROTEÇÃO DE DADOS: (https://www.ccip.pt/pt/newsletter-juris/1241-o-novo-regulamento-de-proteccao-de-dados-parte-vii)

**Hipótese Prática:**  
  
X Lda., Clínica Médica e de Imagiologia que presta consultas e realiza exames médicos pretende actualizar os seus procedimentos em matéria de processamento de dados pessoais, designadamente recolha dos mesmos através da leitura, em leitor apropriado para o efeito, **dos dados pessoais registado no Cartão do Cidadão e, bem assim, prestação do consentimento para acesso aos seus dados de saúde (incluindo exames médicos), por parte de profissionais de saúde.** Como deverá proceder a Clínica X Lda. e quais as diligências a tomar em face do disposto no Novo Regulamento de Dados Pessoais?

**Análise Prática:**  
  
Com efeito, nos termos da al. a) do nº 1 do artigo 6º do Novo Regulamento da Protecção de Dados (doravante NRPD) o tratamento de dados será lícito **se o titular dos seus dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.**  
No caso em apreço, a Clínica X, Lda., pretendendo proceder **à recolha e tratamento de dados pessoais constantes do Cartão do Cidadão dos seus utentes e, bem assim, ao tratamento dos dados relativos à saúde dos mesmos (dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informação sobre o estado da sua saúde)** deverá obter o seu consentimento para tais finalidades.

O consentimento, conforme já nas anteriores newsletters elucidámos, consiste, ao abrigo do NRPD, numa manifestação de vontade, livre, específica, informada e explícita, pelo qual o titular dos dados aceita, **mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento.**

Ora, em face do supra exposto, para efeitos de obtenção de consentimento para o tratamento lícito de dados pessoais e de dados relativos à saúde, **deverá a Clínica X, Lda. preparar declaração de consentimento de tratamento de dados pessoais e de dados relativos à saúde, cujo conteúdo deverá ser facultado e explicado aos utentes e, em caso de concordância dos mesmos, subscrito, através da assinatura, pelos utentes titulares dos dados pessoais a recolher/tratar pela referida Clínica.**

Neste sentido e, tendo em consideração o disposto nos artigos 7º do NRPD, abaixo reproduzimos **sugestão de modelo de consentimento**a implementar no âmbito da hipótese prática apresentada:

(ver)

alertamos, apenas, para a necessidade de **todos os colaboradores administrativos** -não sujeitos a sujeitos a sigilo profissional por força do desempenho de profissões estatutariamente obrigadas a confidencialidade (médicos, enfermeiros) - que acedam e procedam ao tratamento de dados pessoais relativos à saúde dos utentes, **se encontrarem abrangidos por acordo/cláusula de confidencialidade no seu contrato de trabalho, em matéria de dados pessoais, em especial, dados sensíveis, como, efectivamente, é o caso dos dados relativos à saúde dos utentes.**

PROPRIETARIOS DA INFORMAÇÃO:

Perante a lei n.º 12/2005, de 26 de Janeiro, sobre Informação genética pessoal e informação de saúde, a informação de saúde, incluindo os dados clínicos registados, resultados de análises e de outros exames, intervenções e diagnósticos, é propriedade do utente, e as unidades do sistema de saúde são os depositários dessa informação, sujeitos ao segredo médico. Perante isto, o titular da informação tem o direito de tomar conhecimento dessa informação ou de o fazer comunicar algum terceiro indicado por ele, exceto perante circunstâncias devidamente justificadas.

Uma das restrições excecionais nesta matéria, é a informação constante de anotações pessoais efetuadas pelos profissionais de saúde nos registos e processos clínicos dos utentes.

Tratam-se, assim, de anotações pessoais, efetuadas designadamente para memória futura do próprio profissional de saúde, e que não se destinam a classificar ou identificar nenhum dado pessoal do utente.

Tais anotações ou descrições, apesar de poderem eventualmente constar dos registos e processos clínicos dos utentes, não devem ser considerados dados pessoais dos mesmos

do disposto no n.º 1 do artigo 35º da CRP, “Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.”;

QUEM PODE ACEDER AO DADOS:

As decisões da CNPD tem força obrigatória, Pode aceder às instalações, aos sistemas informáticos, a ficheiros de dados pessoais e toda a documentação relacionada. O não acatamento das suas decisões configura crime de desobediência qualificada.

TRATAMENTO DE DADOS:

É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos (tertulia\_1.pdf).

Exceção à proibição desde que: • Haja Consentimento do titular • Exista autorização prevista por lei • Exista interesse público importante (reconhecido pela CNPD) Sempre Com garantias de não discriminação Com medidas de segurança adequadas (tertulia\_1.pdf).

É permitido quando o mesmo for necessário para (tertulia\_1.pdf).:

- medicina preventiva

- diagnóstico médico

- prestação de cuidados ou tratamentos médicos

- gestão de serviços de saúde, desde que:

Seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita a segredo profissional;

Seja notificado e autorizado pela CNPD;

Sejam garantidas medidas adequadas de segurança da informação.

NOVAS TECNOLOGIAS:

Processo clinico eletrónico (tertulia\_1.pdf):

Vantagens:

Facilita a fiscalização pelas autoridades de controlo É mais fácil adotar medidas de segurança da informação Permite adotar níveis diferenciados de acesso à informação Permite a separação lógica entre dados administrativos e de saúde Regista todas as operações de cada um dos utilizadores, responsabilizando-os Permite a obtenção de dados não nominativos para investigação, definição de estratégias de prevenção ou de saúde pública Permite a redução de custos Pode melhorar as condições de trabalho dos profissionais de saúde Pode melhorar a prestação de cuidados ao utente Melhora a proteção de dados

Perigos potenciais:

Enorme quantidade de informação sensível agregada

Aumenta a pressão económica para acesso à informação pelo seu valor

Foge ao controlo dos profissionais de saúde

Pode fragilizar a relação de confiança médico-doente

A adoção de sistemas com deficiente segurança tem consequências imprevisíveis para a saúde e para a privacidade

Eventual integração das entidades detentoras de instituições de cuidados de saúde em grupos económicos (com interesses diversos e por vezes conflituantes) suscita reservas

Particularidades:

- Facilita o acesso independentemente da localização do paciente e do médico

- Aumenta exponencialmente os riscos de segurança

- Contratos “deficientes” de prestação de serviços com empresas detentoras de plataformas

- Back ups da informação – qual a regularidade? onde estão? Na posse do médico ou da empresa? - Estão acauteladas as situações de falências dessas empresas?

- Estão acauteladas as situações de “incumprimento contratual”?

- Estão acauteladas as situações em que não haja acesso à informação?

- As entidades prestadoras dos serviços e detentoras das plataformas informáticas ficam detentoras de uma enorme quantidade de informação (interconexão de informação)

- A localização dos Data Center

- Cloud Computing

- Em países terceiros que não asseguram protecção adequada.

Regulamento de Deontologia Médica n.º 707/2016:

A informação de saúde só pode ser utilizada pelo sistema de saúde nas condições expressas em autorização escrita do seu titular ou de quem o represente.

Os responsáveis pelo tratamento da informação de saúde devem tomar as providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais.

O acesso a informação de saúde pode, desde que anonimizada, ser facultado para fins de investigação.

A gestão dos sistemas que organizam a informação de saúde deve garantir a separação entre a informação de saúde e genética e a restante informação pessoal, designadamente através da definição de diversos níveis de acesso.

O processo clínico só pode ser consultado por médico incumbido da realização de prestações de saúde a favor do doente a que respeita ou, sob a supervisão daquele, por outro profissional de saúde obrigado a segredo e na medida do estritamente necessário à realização das mesmas, sem prejuízo da investigação epidemiológica, clínica ou genética que possa ser feita sobre os mesmos.

O doente tem direito a conhecer a informação registada no seu processo clínico, a qual lhe é transmitida, se requerida, pelo próprio médico assistente ou, no caso de instituição de saúde, por médico designado pelo doente para este efeito.

Sempre que o interesse do doente o exija, o médico deve comunicar, sem demora, a qualquer outro médico assistente, os elementos do processo clínico necessários à continuidade dos cuidados.

O médico pode servir-se do processo clínico para as suas publicações, mas deve proceder de modo a que não seja possível a identificação dos doentes, a menos que expressamente autorizado por escrito a tal pelos próprios doentes ou seus representantes legais.

-- Quando o médico cesse a sua atividade profissional, os seus processos clínicos devem ser transmitidos ao médico que lhe suceda, salvaguardada a vontade dos doentes interessados em que a informação relevante seja transmitida a outro médico por si determinado.

Na falta de médico que lhe suceda, deve o facto ser comunicado à Ordem, por quem receber o espólio do consultório ou pelos médicos que tenham conhecimento da situação, a qual determina o destino a dar-lhes.

O médico assistente que envie um doente a um hospital deve transmitir aos respetivos serviços médicos os elementos necessários à continuidade dos cuidados clínicos. Os médicos responsáveis pelo doente no decurso do seu internamento hospitalar devem prestar ao médico assistente todas as informações úteis acerca do respetivo caso clínico, através de relatório escrito.

Participar prontamente às autoridades de saúde os casos de doenças contagiosas de declaração obrigatória e os casos de doenças contagiosas graves ou de fácil difusão;

Outros:

*handover* como a comunicação oral entre os profissionais de saúde (por ex. enfermeiros) de informação pertinente acerca dos pacientes, sempre que acaba um turno de actividade e um outro começa.

“a transferência de informação (assim como de autoridade e responsabilidade) que acontece no continum de cuidados dos doentes nos momentos de transição e que inclui a oportunidade para levantar questões, clarificar e confirmar” (TeamStepps)

Segundo Kerr 43 o handover tem 3 funções principais: (1) de comunicação expressa, que inclui a informação sobre aspectos objectivos essenciais ao cuidado e o ensino das práticas médicas; (2) de informação encoberta, que integra os elementos psicológicos e sociais dos cuidados (3) de integração cultural, que tem como objectivo a construção da identidade profissional.

Segundo o ERS (Publica\_\_o\_Parecer\_-\_ERS\_016\_2015.pdf):

o desrespeito deste direito de acesso à informação, pode ter consequências imediatas no acesso aos cuidados de saúde – pense-se, por exemplo, no caso de um utente pretender procurar outro prestador de cuidados de saúde e ser-lhe negado o acesso ao seu processo clínico ou a transferência deste para o novo prestador.

O respeito pelo direito de acesso aos cuidados de saúde impõe aos prestadores a obrigação de assegurarem aos seus utentes, os serviços que se dirijam à prevenção, à promoção, ao restabelecimento ou à manutenção da sua saúde, bem como ao diagnóstico, ao tratamento/terapêutica e à sua reabilitação, e que visem atingir e garantir uma situação de ausência de doença e/ou um estado de bemestar físico e mental.

Devendo a informação transmitida ao utente ser verdadeira, completa, transparente, acessível e inteligível pelo seu destinatário concreto2 – cfr. artigo 7º, n.º 2 da Lei n.º 15/2014, de 21 de março.

informação referida deve ser atempadamente transmitida ao utente, para que tenha utilidade e sirva os seus propósitos.

para que a prestação de cuidados de saúde possa ser efetuada com a qualidade, segurança, eficiência e eficácia pretendidas, conforme acima se referiu, é necessário que o profissional de saúde responsável tenha acesso à informação sobre a saúde do utente.

Esta informação sobre o utente é essencial para a elaboração de um diagnóstico sobre o seu estado de saúde e, bem assim, para a definição e eleição da atuação terapêutica mais adequada e apropriada aos objetivos pretendidos.

A informação em causa pode ser recolhida em fontes variadas, desde a mera observação clínica efetuada pelo profissional de saúde ao utente, à prestação de elementos pelo próprio utente ou recolha de dados mais pormenorizados, através de meios complementares de diagnóstico e terapêutica.

cumpre referir que o direito de acesso aos dados de saúde deve ser analisado numa dupla dimensão: sobre a necessidade de proteção da informação de saúde e sobre o âmbito e exercício do direito de acesso à informação.

Conforme acima se afirmou, nos termos do disposto na alínea b) do n.º 2 do artigo 5º dos Estatutos da ERS, aprovados em anexo ao Decreto-Lei n.º 126/2014, de 22 de agosto, “As atribuições da ERS compreendem a supervisão da atividade e funcionamento dos estabelecimentos prestadores de cuidados de saúde no que respeita: […] À garantia dos direitos relativos ao acesso aos cuidados de saúde, à prestação de cuidados de saúde de qualidade, bem como dos demais direitos dos utentes”.

Conforme acima se afirmou, nos termos do disposto na alínea b) do n.º 2 do artigo 5º dos Estatutos da ERS, aprovados em anexo ao Decreto-Lei n.º 126/2014, de 22 de agosto, “As atribuições da ERS compreendem a supervisão da atividade e funcionamento dos estabelecimentos prestadores de cuidados de saúde no que respeita: […] À garantia dos direitos relativos ao acesso aos cuidados de saúde, à prestação de cuidados de saúde de qualidade, bem como dos demais direitos dos utentes”

os dados de saúde reportam-se à esfera de vida pessoal e íntima de cada cidadão, requerendo do ordenamento jurídico um nível de proteção mais exigente

**Para que os utentes possam fornecer ao prestador de cuidados de saúde todos os elementos que este necessita para melhor exercer a sua atividade, terão de confiar que a informação será utilizada apenas para essa finalidade.**

No âmbito do segredo profissional, está em causa a proteção de um bem jurídico fundamental, que justifica inclusivamente a previsão de um tipo legal de crime: nos termos do disposto no artigo 195º do Código Penal, pode ler-se que,

“Quem, sem consentimento, revelar segredo alheio de que tenha tomado conhecimento em razão do seu estado, ofício, emprego, profissão ou arte é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.”.

Assim, nos termos do disposto na alínea c) do n.º 1 do artigo 43º da LPD, “É punido com prisão até um ano ou multa até 120 dias quem intencionalmente: […] c) Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização”, sendo certo que, por se tratarem de dados de saúde, as penas são agravadas para o dobro dos limites referidos, atento o disposto n o n.º 2 do mesmo artigo 43º.

Nos termos do n.º 1 do artigo 44º da LPD, “Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado é punido com prisão até um ano ou multa até 120 dias.”.

Nos termos do n.º 1 do artigo 45º da LPD, “Quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afectando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias.”.

diz respeito à obrigação de sigilo profissional, afirma-se no n.º 1 do artigo 47º da LPD o seguinte: “Quem, obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com prisão até dois anos ou multa até 240 dias.”.

termos da alínea e) do n.º 3 do artigo 31º do Decreto-Lei n.º 131/2014, de 29 de agosto (que regulamenta a Lei n.º 12/2005, no que se refere à proteção e confidencialidade da informação genética, às bases de dados genéticos humanos com fins de prestação de cuidados de saúde e investigação em saúde), “Constitui contraordenação punível com coima no montante mínimo de € 2 500 e máximo de € 3 740, no caso das pessoas singulares, e no montante mínimo de € 10 000 e máximo de € 30 000, no caso das pessoas coletivas: […] e) A divulgação a terceiros de informação genética relacionada com a saúde do respetivo titular, fora dos casos previstos na Lei n.o 67/98, de 26 de outubro, em violação do disposto no n.º 1 do artigo 20.º”.

Todas as informações obtidas pelos profissionais de saúde no exercício das suas funções estão inseridas naquela esfera da intimidade privada do utente - este é que é, para todos os efeitos, o titular do direito às mesmas.

Como forma de acautelar o acesso de terceiros a informações abrangidas pelo dever de confidencialidade, de acordo com o disposto neste artigo 4.º, podem os estabelecimentos prestadores de cuidados de saúde separar a informação contida no seu processo clínico, entre informação de saúde e a restante informação pessoal, podendo estabelecer mecanismos de controlo de acesso mais apertados, no caso da informação em saúde, e menos restritivos, no caso da restante informação pessoal;

O que poderá permitir, por exemplo, que os funcionários dos estabelecimentos prestadores de cuidados de saúde que não sejam profissionais de saúde não devam ter acesso à informação em saúde contida em processo clínico (dados clínicos registados, resultados de análises, e outros exames subsidiários, intervenções e diagnósticos), mas possam ter acesso à restante informação pessoal (por exemplo, o nome, a morada, o número da segurança social, o número de contribuinte, o número do bilhete de identidade, o número de beneficiário de subsistema de saúde ou de seguro de saúde, bem como a identificação dos atos ou exames praticados ao utente).

vantagens na criação e manutenção dos processos clínicos: melhora a qualidade dos cuidados a prestar; contribui para evitar o erro médico; torna mais rápido o acesso à informação; facilita a comunicação e partilha de informação entre profissionais de saúde e estabelecimentos; e constitui um meio de prova, em caso de conflito entre os intervenientes.

Com interesse para o objeto do presente parecer, importa referir que a LPD define, como regra, a proibição do tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos, exceto quando tal “for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efectuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação.” (cfr. n.º 1 e 4 do artigo 7º da LPD).

Portanto, a regra é a da proibição do tratamento de dados de saúde, exceto quando tal atividade tiver como propósito a prestação de cuidados de saúde.

<http://www.atlasdasaude.pt/publico/content/comissao-de-etica-demarca-se-de-proposta-sobre-venda-de-dados>

Segunda, 3 Julho, 2017 - 10:54

A recomendação de compra e venda de dados em saúde, com o consentimento informado dos doentes, para que possam ser utilizados em respostas a necessidades concretas, foi divulgada em comunicado pelos promotores da iniciativa e comentada pela presidente do ‘Health Parliament Portugal' (HPP), Ana Castro

Numa declaração escrita, a Comissão de Ética, uma das seis comissões que integram o HPP, "demarca-se totalmente desta visão" e divulga as recomendações apresentadas, em que sugeriu, sobre este assunto, "salvaguardar, em legislação, a exigência clara e transparente da finalidade do uso dos dados em saúde e a retribuição ao cidadão".

Segundo um comunicado do Parlamento da Saúde, as recomendações preveem a criação de “um modelo que permita aos cidadãos partilharem os seus dados em saúde através de um consentimento informado para que os mesmos possam ser utilizados em resposta a necessidades concretas” e uma proposta para “legislar a cedência ou venda de dados em saúde e investir as receitas” no SNS.

a presidente do HPP adiantou que há propostas relacionadas "com a partilha, a proteção dos dados e a valorização dos dados em saúde" que são transversais aos grupos das tecnologias de informação, da ética e do doente no centro da decisão

Para os “deputados” da Comissão de Ética, as posições da presidente do HPP acerca de venda de dados "refletem somente e apenas a sua opinião pessoal ou um equívoco de interpretação".

Os sete membros da Comissão de Ética, proveniente das áreas de economia, finanças, ética, medicina, farmácia e investigação científica, são contra a posição da presidente do HPP de que "teria de ser feito um contrato entre o doente e a empresa, como um outro qualquer contrato de compra de um bem. O doente ou recebe ou abdica do dinheiro para o SNS ou para a instituição que for".

A Comissão entende ainda que "o consentimento do cidadão, na decisão de partilhar os seus dados, deverá respeitar os seus interesses, quando legítimos", defendendo ainda que "deverá ser respeitada a autonomia, dignidade e privacidade, devendo existir como pressupostos gerais dos dados em saúde a ocultação da identidade e limites à reidentificação".

TERMINOLOGIA:

**Informação médica:** informação de saúde destinada a ser utilizada em prestações de cuidados ou tratamentos de saúde (\_\_\_Regulamento n.pdf).

**Informação de saúde:** todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar (Consolidação\_106487526\_28-04-2017.pdf).

**Processo clínico:** qualquer registo, informatizado ou não, que contenha informação de saúde sobre doentes ou seus familiares. Este deve conter toda a informação médica disponível que diga respeito ao doente (\_\_\_Regulamento n.pdf).

o processo clínico relativo a um determinado utente/doente deve conter informação suficiente sobre a sua identificação, bem como sobre todos os factos relacionados com a sua saúde, incluindo a sua situação actual, evolução futura e história clínica e familiar, e ainda com os factos relacionados com os cuidados de saúde que lhe tenham sido prestados e que lhe venham a ser prestados no estabelecimento de saúde em que o processo clínico se encontra depositado. Entre os elementos que devem integrar o processo clínico refiram-se: i) a memória de anamnese (entrevista prévia ao paciente); ii) o registo da admissão (e o estado de saúde do doente nesse momento); iii) o diagnóstico e os tratamentos utilizados (incluindo os resultados dos exames e das análises); iv) os fármacos, produtos e outros materiais utilizados (e respectiva dosagem, lote, marca e outros elementos relevantes); v) a evolução do seu estado de saúde, informação prestada ao doente sobre o seu estado de saúde e eventuais correspondências entre profissionais (ou mesmo a mudança de profissionais que se encontrem a cuidar dos doentes); vi) a transferência dos utentes de serviços; vii)o prognóstico; viii) o registo de alta dos doentes; e ainda ix) os custos e a facturação subjacente a todos os actos incluídos na prestação de cuidados de saúde.”. (Publica\_\_o\_Parecer\_-\_ERS\_016\_2015.pdf)

**Processo Clínico Eletrónico:** Agrega informação dispersa Permite a articulação entre os vários serviços e entre os vários níveis de cuidados de saúde Permite o pedido em tempo real de meios complementares de diagnóstico e consulta de resultados A circulação da informação é automática Facilita a medicina partilhada entre o utente, profissionais de saúde e entidades prestadoras de serviços de Saúde (tertulia\_1.pdf)

Um processo clínico electrónico pode conter os dados relativos à história clínica, exame físico, evolução no internamento, diagnósticos, intervenções cirúrgicas, introduzidos e visualisados de forma estruturada, bem como resultados de exames complementares de diagnóstico, imagem (raios X, ecografia) ou sinal (electrocardiograma, cardiotografia).

**Ficha clínica:** é o registo dos dados clínicos do doente, das anotações pessoais do médico e tem como finalidade a memória futura e a comunicação entre os profissionais que tratem o doente (\_\_\_Regulamento n.pdf).

**Dados pessoais:** qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social (resumir) (Publica\_\_o\_Parecer\_-\_ERS\_016\_2015.pdf e tertulia\_1.pdf).

**Tratamento de dados pessoais:** qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição (resumir) (Publica\_\_o\_Parecer\_-\_ERS\_016\_2015.pdf).

(367969507b2209c94a4b23992a50d425dfab.pdf)

**dados anonimizados** - alteração da PHI que torna impossível vincular indivíduos com seus dados (367969507b2209c94a4b23992a50d425dfab.pdf).

**dados de-identificados** - a eliminação de todos os identificadores como enumerados sob HIPAA pelo método de porto seguro (ou seja, nome do paciente, número de registro médico, número de segurança social, e outros campos de dados que apontam diretamente um paciente aos seus dados). Existe potencialmente outra abordagem que envolve ter um estatístico para determinar que a capacidade (probabilidade) de poder combinar dados com outras fontes públicas de informação e identificar com sucesso um indivíduo é extremamente pequena (367969507b2209c94a4b23992a50d425dfab.pdf).

**dados anonimatos reversíveis** - a alteração da PHI de forma que a re-identificação possa ser realizada através do acesso a uma chave protegida que permita vincular indivíduos com seus dados somente através de um intermediário confiável (367969507b2209c94a4b23992a50d425dfab.pdf).

**Comissão Nacional de Protecção de Dados (CNPD):** Entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República. Tem como atribuição controlar e fiscalizar o cumprimento das disposições legais em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.

**Ordem dos Médicos:** associação pública representativa dos médicos que exercem a profissão em Portugal, com cerca de 47.000 membros, distribuídos por especialidades, subespecialidades e competência, cuja principal missão é promover a defesa da qualidade dos cuidados de saúde prestados à população, bem como o desenvolvimento, a regulamentação e o controlo do exercício da profissão de médico, assegurando a observância das regras de ética e deontologia profissional.

**Privacidade** diz respeito ao direito fundamental de cada **indivíduo** de decidir quem deve ter acesso aos seus dados pessoais (<http://im.med.up.pt/seguranca/index.html>).

**Confidencialidade** trata de ter disponível **medidas e mecanismos** para manter a privacidade do indivíduo, proporcionando uma estrutura que permita dar acesso a informação privada, a quem foi dada autorização para tal (<http://im.med.up.pt/seguranca/index.html>).

PROTOCOLOS DE COLABORAÇÃO:

(PROTOCOLO DE COOPERAÇÃO ENTRE O GABINETE NACIONAL DE SEGURANÇA / CENTRO NACIONAL DE CIBERSEGURANÇA E A SPMS – SERVIÇOS PARTILHADOS DO MINISTÉRIO DA SAÚDE, E.P.E.)

O GNS/CNCS tem como principal objetivo contribuir para que o país use o ciberespaço de forma livre, mas, e acima de tudo, de forma confiável e segura, através da promoção de uma contínua melhoria da cibersegurança nacional e da cooperação internacional, bem como da implementação de medidas e instrumentos necessários para antecipar, detetar, reagir e recuperar de situações que, face à ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

O SPMS tem com principal objetivo a cooperação, a partilha de conhecimento e informação e o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas e tecnologias de informação e de comunicação, garantindo a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde.

Dados as competências particulares e objetivos comuns, no passado dia 21 de fevereiro de 2017, o SPMS assinou com o GNS/CNCS um protocolo de cooperação. Este protocolo visa promover a otimização de procedimentos e uma maior eficiência no sistema, estabelecendo as formas de cooperação entre as partes no desenvolvimento das capacidades nacionais de cibersegurança, troca de conhecimento e aprofundamento das capacidades.

A SPMS desenvolveu o **IT Security Assessment** de Segurança TIC na Administração Pública para auxiliar e dar suporte aos administradores governamentais, responsáveis de TIC e responsáveis departamentais na compreensão da magnitude das ameaças e das mudanças necessárias para proteger os seus organismos e os seus programas de atuação.  Esta ferramenta consiste numa framework com cinco dimensões — visão, gestão de risco, pessoas, processos e tecnologias de segurança.

COMPARAÇÃO COM A PALESTRA SOBRE PROTEÇÃO DE DADOS:

*Fonte: Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*:

Assim como os dados singulares, os dados médicos, devem … Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimente do comércio e o bem-estar dos indivíduos;

Considerando que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social - em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença - e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia, estabelecer garantias adequadas e específicas para a protecção dos direitos fundamentais e da vida privada das pessoas;

Tratamento de dados:

Comparando com os dados pessoais, os dados médicos são semelhantes [ver melhor as semelhanças].

Artigo 37.º do Regulamento\_707\_2016

Tratamento da informação da saúde

1 — Os responsáveis pelo tratamento da informação de saúde devem tomar as providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais.

2 — As unidades do sistema de saúde devem impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respetivas cópias de segurança, assegurando os níveis de segurança apropriados e cumprindo as exigências estabelecidas pela legislação que regula a proteção de dados pessoais, nomeadamente para evitar a sua destruição, acidental ou ilícita, a alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação.

3 — A informação de saúde só pode ser utilizada pelo sistema de saúde nas condições expressas em autorização escrita do seu titular ou de quem o represente.

4 — O acesso a informação de saúde pode, desde que anonimizada, ser facultado para fins de investigação.

5 — A gestão dos sistemas que organizam a informação de saúde deve garantir a separação entre a informação de saúde e genética e a restante informação pessoal, designadamente através da definição de diversos níveis de acesso.

6 — A gestão dos sistemas de informação deve garantir o processamento regular e frequente de cópias de segurança da informação de saúde, salvaguardadas as garantias de confidencialidade estabelecidas por lei.

O chamado «responsável pelo tratamento dos dados», que é a pessoa ou entidade que trata os seus dados, tem de cumprir as regras da UE aplicáveis ao tratamento e armazenamento dos seus dados pessoais (<https://europa.eu/youreurope/citizens/consumers/telecoms-internet/data-protection-privacy/index_pt.htm>):

* os seus dados só podem ser tratados para **fins legítimos e claramente definidos**
* não lhe podem solicitar demasiados dados
* os dados que permitam a sua identificação individual (por exemplo, nome ou dados de contacto) não podem ser conservados durante mais tempo do que o necessário
* deve poder **corrigir, apagar ou bloquear** os seus dados pessoais
* os seus **dados devem ser protegidos** contra a destruição, perda e alteração acidentais ou ilícitas e a divulgação

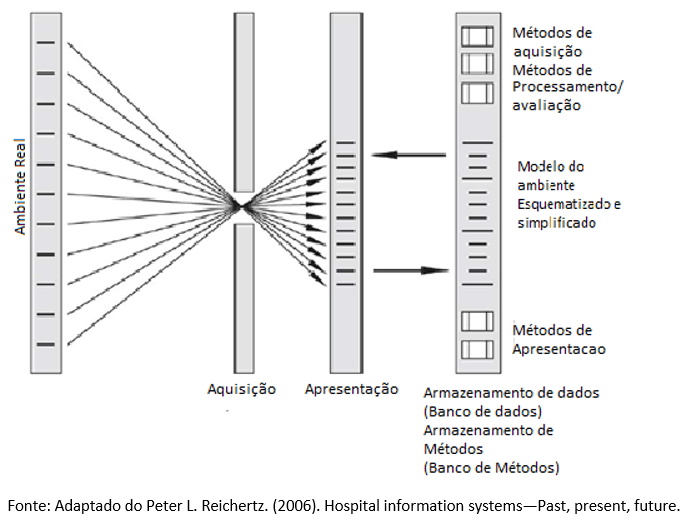
Em certos casos, tem o direito de **exigir que os responsáveis pelo tratamento dos dados corrijam, apaguem ou bloqueiem dados sobre si que estejam incorretos** Trata-se do chamado «direito ao esquecimento».

CLONCLUSÕES

Problemas de comunicação entre os profissionais de saúde têm sido associados, em vários estudos, à diminuição de qualidade de cuidados e a mortes por erros médicos que poderiam ser evitados.

os estabelecimentos prestadores de cuidados de saúde, de assegurar a confidencialidade de todas as informações contidas nos processos clínicos dos utentes, nomeadamente mediante a adoção de mecanismos que garantam a segurança das instalações ou dos meios informáticos, consoante as mesmas se encontrem contidas sem suporte de papel ou suporte informático;

IMAGENS:



PLATAFORMAS / SOFTWARES EXISTENTES:

A evolução do exercício da Medicina, nomeadamente com a chegada das novas tecnologias obriga os Médicos a uma constante actualização.

A prescrição electrónica de medicamentos e meios complementares de diagnóstico e terapêutica (MCDT’s), garantida que esteja a segurança do trânsito de dados, representa um passo importante na monitorização e controlo do uso dos recursos em Saúde.

Plataforma de Dados da Saúde (PDS) (<http://spms.min-saude.pt/2013/11/pds-plataforma-de-dados-da-saude/>):

* nível nacional
* permite o registo e partilha de informação clínica
  + pode ser acedida pelos diferentes agentes da prestação de cuidados (utentes, proﬁssionais do SNS e de fora do SNS), através do número de utente do SNS.
* Oacessoaestesdadosérealizadoatravés de Portais, a partir das instituições locais onde são guardados.
  + Os portais de interesse fundamental são: o Portal do Utente, onde cada utente pode registar os seusdadosdesaúde,agendarconsultas,comunicarcomoseumédico,etc;oPortaldoProﬁssional, que permite aos proﬁssionais de saúde o acesso aos dados clínicos dos doentes, armazenados nos servidores de cerca de 400 instituições e de cinco bases de dados centrais, cobrindo todos os cuidados de saúde primários e todos os hospitais públicos.

Paralelamente, foi desenvolvido um projeto a nível europeu de eSaúde: o epSOS.

“O epSOS pretende contribuir para a melhoria da qualidade dos cuidados de saúde prestados aos cidadãos europeus quando estão fora do seu país, permitindo que os proﬁssionais de saúde dos outros países participantes acedam à sua informação clínica, residente no seu país de origem [20].” (DiogoSebe\_SistemaInformacaoEmergenciaMedica.pdf)

Oobjetivoprincipalresume-seàpartilhatransfronteiriçadeinformaçãoclínicadoutente(seja como turista, em viagem de negócios, estudantes ou trabalhadores nas zonas transfronteiriças), entre os países envolvidos no projeto, dos quais Portugal já faz parte. A informação que pode ser acedida divide-se em: Resumo Clínico (quer por Médicos, quer por Utentes ), Prescrição Eletrónica, relatório dos cuidados de saúde prestados (HCER) e relatórios de medicação (MRO).

(ACORDO Ordem dos Médicos / iMED) (<http://ordemdosmedicos.pt/wp-content/uploads/2017/09/Protocolo_IMED.pdf>)

O iMED, com 17.000 médicos aderentes, é uma plataforma de gestão clínica on-line rápida e simples, com altos níveis de eficiência. Esta plataforma de excelência reúne num único software, todas as ferramentas essenciais para um pleno e eficiente funcionamento de um consultório ou clinica.

O sistema funciona em tecnologia totalmente web, sem necessidade de configuração ou instalação, permitindo-lhe com apenas uma ligação à internet aceder ao sistema a qualquer altura, em qualquer lugar.

Tratamento de dados

1. O responsável pelo tratamento de dados é o iMED;
2. O iMED obriga-se a respeitar e a respeitar a confidencialidade dos dados que recolhe.
3. O iMED obriga-se a tratar de acordo com as normas legais em vigor, de forma informatizada ou sem meios automáticos, todos os dados recolhidos por intermédio do software que disponibiliza, nomeadamente, as normas legais estabelecidas pela Comissão Nacional de Proteção de Dados, de modo a não divulgar, ceder, transmitir ou facultar os dados a que tem acesso.
4. O iMED, por intermédio de informações e alertas, dará a conhecer aos utilizadores medidas para que seja garantido a estes um nível de segurança adequado aos riscos que os meios de comunicação à distância apresentam;
5. Entre outras obrigações, a iMED obriga-se a:
   1. Permitir ao titular dos dados, gratuitamente, o acesso e a correção das informações prestadas assim como a destruição dos dados recolhidos.
   2. Não utilizar os dados recolhidos para finalidade estranha ao objeto deste protocolo, nomeadamente para serem utilizados por terceiros para fins que não os previstos no presente protocolo;
   3. Ter sistemas de segurança que impeçam a consulta, modificação, destruição ou acrescentamento dos dados por pessoa não autorizada a fazê-lo e que permitam detetar desvios de informação;
   4. Respeitar o sigilo profissional em relação aos dados tratados;
   5. Não realizar qualquer tipo de interconexão de dados ou tratamento estatístico.
6. O iMED obriga-se a indemnizar os lesados pelos danos causados na eventualidade de violar as obrigações a que se encontra adstrito assim como a assumir qualquer tipo de responsabilidade do foro contraordenacional, civil e criminal na sequência dessa mesma violação.

Objectivo do Acordo de Parceria

Disponibilização da Plataforma de Prescrição Médica Eletrónica iMED, tendo em vista a obrigatoriedade legal da utilização de plataformas informáticas para prescrição eletrónica de medicamentos.

(<https://www.imed.pt/imed/>)

O iMED é o mais simples e completo software de gestão clínica, que assiste na prescrição eletrónica de medicamentos e em todas as tarefas que compõem a atividade profissional médica. Esta solução integrada dispõe de todas as ferramentas e módulos essenciais para a gestão de espaços na área da saúde, necessários para um serviço mais rápido e eficiente.

* Tecnologia totalmente web, alojada na Cloud;
* Dispõe de aplicação móvel
* Ligação instantânea ao Registo Nacional de Utentes (RNU);
* Serviço de apoio presencial e/ou telefónico gratuito;
* Diferentes níveis de acesso para o staff médico e administrativo;
* Prescrições: Emita prescrições de medicamentos em apenas 15 segundos.
* Ficha Clínica: Consulte e mantenha a informação clínica dos seus pacientes atualizada e organizada.
* Vídeo Consultas: Acompanhe os seus pacientes e rentabilize o seu tempo através das vídeo consultas.
* Requisições: Emita requisições de MDCT's para o SNS ou qualquer outro subsistema.
* Consultas: Agende, consulte e organize as suas consultas de uma forma rápida e prática.
* Alertas SMS: Reduza ausências ou situações de atraso na sua agenda.
* Declarações: Simplifique e automatize a emissão das suas declarações e atestados médicos.  
  Faturação: Evite surpresas e acompanhe permanentemente os custos da sua clínica ou consultório.
* iMED Mobile: Prescreva com o seu telemóvel ou tablet, a partir de qualquer lugar.

PROTOCOLO DE COOPERAÇÃO ENTRE MedicineOne E A ORDEM DOS MÉDICOS (<http://ordemdosmedicos.pt/wp-content/uploads/2017/09/Protocolo_MedicineOne.pdf>)

1. O My MedicineOne é uma aplicação de gestão clínica.

Tem as seguintes funcionalidades:

* Gestão do ficheiro de utentes • Prescrição Electrónica de Medicamentos • Gestão de Patologias dos utentes • Gestão de alergias dos utentes • Registo de Consultas (SOAP) • Simposium Terapêutico • Gestão de Tarefas • Correio Interno • Configuração Simplificada

CLÁUSULA 5.ª

Tratamento de dados

1. O responsável pelo tratamento de dados é a MedicineOne.
2. A MedicineOne obriga-se a respeitar e a proteger a confidencialidade dos dados que recolhe.
3. A MedicineOne obriga-se a tratar de acordo com as normas legais em vigor, de forma informatizada ou sem meios automáticos, todos os dados recolhidos por intermédio do software que disponibiliza, nomeadamente, as normas legais estabelecidas pela Comissão Nacional de Proteção de Dados, de modo a não divulgar, ceder, transmitir ou facultar os dados a que tem acesso.
4. A MedicineOne, por intermédio de informações e alertas, dará a conhecer aos utilizadores medidas para que seja garantido a estes um nível de segurança adequado aos riscos que os meios de comunicação à distância apresentam;
5. Entre outras obrigações, a MedicineOne obriga-se a:
   1. Permitir ao titular dos dados, gratuitamente, o acesso e a correção das informações prestadas assim como a destruição dos dados recolhidos.
   2. Não utilizar os dados recolhidos para finalidade estranha ao objeto deste protocolo, nomeadamente para serem utilizados por terceiros para fins que não os previstos no presente protocolo;
   3. Ter sistemas de segurança que impeçam a consulta, modificação, destruição ou acrescentamento dos dados por pessoa não autorizada a fazê-lo e que permitam detetar desvios de informação;
   4. Respeitar o sigilo profissional em relação aos dados tratados;
   5. Não realizar qualquer tipo de interconexão de dados ou tratamento estatístico.
6. A MedicineOne obriga-se a indemnizar os lesados pelos danos causados na eventualidade de violar as obrigações a que se encontra adstrito assim como a assumir qualquer tipo de responsabilidade do foro contraordenacional, civil e criminal na sequência dessa mesma violação.

(<http://www.medicineone.net/>)

A MedicineOne é uma empresa tecnológica de origem portuguesa e vocação mundial, dedicada ao desenvolvimento de software para o mercado da saúde. A nossa solução de gestão clinica é ao mesmo tempo uma das mais antigas, inovadoras e completas do mundo. Desenvolvemos uma das melhores soluções de sotware para gerir pequenas e grandes unidades de saúde, sistemas de saúde públicos e privados em instalações onsite ou cloud computing. Começámos em Portugal, mas já estamos em 4 continentes. Levamos connosco a inovação, a engenharia, a excelência e a paixão portuguesas. Competimos com os melhores e não nos damos nada mal...

O MedicineOne encontra-se desenhado para agilizar os processos dentro de qualquer organização, permite aos médicos e a todos os profissionais de saúde, a partilha de dados, preparado para reduzir o risco de erro.

O MedicineOne está apto para gerir toda e qualquer unidade de saúde.

tem acesso a:

* Prescrição de medicamentos
* Gestão de patologias
* Consultas (SOAP)
* Hábitos
* Referênciação
* Atos médicos
* Faturação
* Correio interno
* Agendas e salas de espera
* Análises e MCDT's
* Biometrias
* Antecedentes
* Fichas de especialidade
* Cessação tabágica
* Simposium
* Tarefas
* Suporte
* Atestado para Carta de Condução

aplicações informáticas em uso no CHMA: SAM, SAPE e ALERT

<http://spms.min-saude.pt/product/sclinicocsp/>

<https://comunidade.mysns.pt/missao.html>

<http://spms.min-saude.pt/product/area-cidadao/>

<http://epr.med.up.pt/intensive/index.html>:

O acesso está condicionado a autorização do sistema (login e password) - segurança, confidencialidade e privacidade

Vários utilizadores podem aceder em simultâneo à informação clínica, esta pode ser acedida remotamente.

Por outro lado, desde que a informação esteja estruturada podem ser feitas análises estatísticas diversas ou pesquisas dos dados clínicos

(<http://spms.min-saude.pt/product/rnu/>)

**RNU – Registo Nacional de Utentes**  
O Registo Nacional de Utentes constitui a base de dados de referência para a identificação dos Utentes do Serviço Nacional de Saúde, ao nível de um Master Patient Index (através do número de Utente), sendo constituído atualmente por três grandes componentes:

* Base de dados nacional (repositório central de dados dos Utentes do SNS);
* Aplicação Web (WEBRNU) para gestão dos dados de identificação dos Utentes;
* Plataforma de interoperabilidade, disponibilização serviços de consulta de dados (Web Services)

O RNU é alimentado pela interação direta dos administrativos dos Cuidados de Saúde Primários e dos Hospitais do SNS (limitado) através do WebRNU, pelos processos do Cartão de Cidadão (CC) e pela integração de dados com as Regiões Autónomas da Madeira e dos Açores.  
Os dados de identificação do cidadão são recolhidos no momento da sua requisição, nas instituições competentes (conservatórias do registo civil, p.e.). Estes dados são enviados para o RNU através de Web Services, disponíveis para o efeito. O RNU disponibiliza, através dos serviços de consulta – Web Services, dados dos Utentes a um vasto número de entidades e sistemas do SNS, devidamente autorizados para o efeito.

(<http://spms.min-saude.pt/product/area-cidadao/>)

O Registo de Saúde Electrónico (RSE) – visa a reunir informação essencial de cada Cidadão para a melhoria da prestação de cuidados de saúde; o RSE é construído por dados clínicos recolhidos electronicamente para cada Cidadão e produzidos por entidades que prestam cuidados de saúde.

O RSE permite o registo e partilha de informação clínica entre o utente, profissionais de saúde e entidades prestadoras de serviços de Saúde, de acordo com os requisitos da Comissão Nacional de Proteção de Dados (Autorização n.º 940/2013).

É constituída por quatro portais, seguros e contextualizados: Área do Cidadão; Portal do Profissional; Portal Institucional e Portal Internacional.

* Área do Cidadão: destinado aos utentes com o objetivo de melhorar a qualidade dos serviços prestados, este passa a ter um papel ativo na manutenção, promoção e melhoria do seu estado de saúde e, consequentemente, um atendimento mais eficaz e seguro. Após autenticação no portal permite, o registo de contactos de emergência, de informação sobre hábitos, medicação, alergias e doenças, das medições de peso, altura, glicémia, tensão arterial, colesterol, triglicéridos, saturação de oxigénio e de tempo de coagulação do sangue(INR), carregar documentos de saúde, partilhar dados de saúde com os profissionais de saúde do SNS, contacto direto com o seu centro de saúde, marcação online de consulta, pedido de prescrição de medicação crónica, consultas a informações médicas e c onsulta dos dados que constam do Resumo Clínico Único (RCU): alergias, medicação, diagnósticos, cirurgias e vacinação.
* Portal do Profissional: plataforma **centrada no utente** que permite aos profissionais de saúde (médicos e enfermeiros) terem **acesso à informação clínica do utente**. A informação que o utente disponibiliza na Área do Cidadão e que, posteriormente, autoriza a sua consulta, permite ao profissional de saúde obter alguns indicadores que o podem auxiliar a um **melhor conhecimento, diagnóstico e tratamento** do mesmo. Permite também, cronograma com todos os contactos efetuados pelo utente, nas diversas instituições do país, Informação partilhada pelo utente na Área do Cidadão, Resumo de Saúde Oral e visualização das prescrições de medicamentos emitidas.
* Portal Institucional: **backoffice** para gestão centralizada do RSE e **estatísticas** referentes ao RSE. Prevê-se a criação de um repositório de informação clínica anonimizada, residente na DGS, para fins de **saúde pública** e **investigação epidemiológica**.
* Portal Internacional: permite que um médico de outro país da União Europeia consulte o **Resumo Clínico Único** do utente, mediante a sua autorização prévia no portal.

APOSTAS FUTURAS/RECENTES:

<http://www.atlasdasaude.pt/publico/content/coimbra-recebe-centro-de-formacao-em-ciberseguranca-na-saude>

Henrique Martins, presidente dos Serviços Partilhados do Ministério da Saúde (SPMS), ggcuja Academia assinou ontem um protocolo com o Centro Hospitalar e Universitário de Coimbra (CHUC) para a criação do Centro de Desenvolvimento e Capacitação em Cibersegurança na Saúde, destacou a localização de Coimbra no centro do país "a meia distância" das universidades às quais se destina o polo de formação.

Por outro lado, a Academia SPMS pretende que o Centro Hospitalar e Universitário de Coimbra passe a desempenhar um papel "fundamental" na investigação da cibersegurança de dispositivos clínicos - quer em termos de ‘hardware’, quer no ‘software’ utilizado - os quais, embora sejam rotulados de seguros ao nível da cibersegurança aquando da sua produção, "têm de ser experimentados".

 o presidente do conselho de administração do CHUC, Fernando Regateiro, garantiu que a instituição quer "dar o salto, com segurança, cautela e de uma forma determinada" para possuir o mesmo sistema em todos os espaços do centro hospitalar.

O Centro de Desenvolvimento e Capacitação em Cibersegurança na Saúde pretende, entre outros objetivos e no âmbito do protocolo hoje assinado, contribuir para a divulgação para todo o Serviço Nacional de Saúde das melhores práticas em cibersegurança, promover a formação e capacitação em tecnologias de informação e cibersegurança para profissionais de saúde e também integradas em currículos de universidades e politécnicos e apoiar o desenvolvimento de inovações tecnológicas em matéria de ciberdefesa relevante aos riscos próprios da saúde.

<http://www.90segundosdeciencia.pt/episodes/ep-274-pedro-rodrigues/>

Pedro Pereira Rodrigues, investigador no [CINTESIS](http://cintesis.eu/) – Centro de Investigação em Tecnologias e Serviços de Saúde e docente na Faculdade de Medicina da Universidade do Porto ([FMUP](https://sigarra.up.pt/fmup/pt/web_page.inicial)), está a desenvolver este projeto em consórcio com o [INESC TEC](http://www.inesctec.pt/).

“O [NanoSTIMA](http://cintesis.eu/portfolio-items/nanostima/) tem como objetivo global a capacidade de medição, de recolha e de integração de todo o tipo de dados de saúde e de doença da população, para desenvolver novos métodos de análise desses dados, para respondermos às perguntas de investigação que habitualmente já tentamos responder com os métodos mais tradicionais de investigação clínica e de investigação em saúde”, explica.

Pedro Pereira Rodrigues aponta como objetivo final do projeto a possibilidade de no futuro termos produtos que, integrando dados de múltiplas fontes, como sensores, dados administrativos de interação dos indivíduos com o sistema nacional de saúde, ou dados clínicos recolhidos de cada indivíduo, possam ser usados quer pelos investigadores, quer pelos profissionais de saúde.

Estes dados podem depois ser usados para determinar se uma pessoa deve ou não ser observada, prever qual a progressão de uma doença, ou até mesmo sugerir qual a intervenção mais indicada para cada paciente.

Neste Momento, o NanoSTIMA encontra-se ainda numa fase de desenvolvimento de conhecimento fundamental para que estes sistemas sugeridos possam um dia fazer parte do nosso quotidiano.

O NanoSTIMA – Macro-to-Nano Human Sensing: Towards Integrated Multimodal Health Monitoring and Analytics é um projeto financiado pelo N2020 em cerca de 7,2 milhões de euros, dos quais aproximadamente 1,4 milhões são geridos pelo CINTESIS.

Organizado em cinco linhas de investigação, o NanoSTIMA visa o desenvolvimento de competências científicas que permitam fazer face aos grandes desafios colocados pela revolução a que assistimos na área da saúde e do bem-estar e que aponta para a progressiva utilização de nanossensores, alguns dos quais implantáveis no corpo humano, para monitorização de múltiplos indicadores, numa lógica de promoção da saúde e prevenção da doença. Este projeto aborda também questões como a integração e aplicação de dados pessoais de diferentes fontes.

Pedro Pereira Rodrigues, investigador principal do grupo BioData, lidera o projeto NanoSTIMA no CINTESIS, em conjugação com vários parceiros, designadamente o INESC TEC, o IT e o CIDESD.

Estamos à beira de uma grande revolução na forma como nossa saúde e bem-estar é gerenciada desde que a cirurgia asséptica se tornou amplamente disponível há cerca de 100 anos.

Hoje, a tecnologia médica e de consumo está convergindo para oferecer um novo paradigma para o "auto-monitoramento" contínuo, dia e noite, à medida que os sensores fisiológicos estão ficando tão pequenos, wearable e até implantáveis.

que vamos esquecer que os estamos carregando / em nosso corpo. Essa revolução de detecção humana Macro-a-Nano acontecerá nos próximos anos, simplesmente não sabemos exatamente quantos anos serão necessários.

No presente projeto, imaginamos um futuro onde os humanos estarão usando, dentro e em seu corpo, dezenas de micro e nano sensores que acompanharão uma grande quantidade de indicadores fisiológicos de nosso fantástico corpo sofisticado. Esses indicadores permitirão a revolução acima mencionada e fornecerão a possibilidade de se deslocar do atual paradigma de saúde aguda (onde a cirurgia é o máximo exponente) para um medicamento preventivo que atua o mais cedo possível para gerenciar problemas de saúde e bem-estar.

Os futuros sistemas de detecção humana serão redes multi-camadas de dispositivos sensores e atuadores, variando da macro ao nano. Os ecossistemas de dispositivos pequenos interoperáveis ​​nessas diferentes camadas irão trocar dados e comandos perfeitamente para nos conscientizarmos da nossa saúde, agir mais cedo para possíveis sinais de doenças e seguramente direcionar nossa sociedade para um menor custo de saúde.

Além disso, esse paradigma imaginado transformará nossa sociedade mais preparada para o envelhecimento da população demográfica que já é uma certeza para os próximos 50 anos.

No entanto, há dois desafios principais a serem abordados para que esse paradigma imaginado se torne uma realidade:

Evolua a partir da macro de hoje para tecnologias de detecção de micro e nano humanos do futuro, que serão a pedra angular da revolução que vai desencadear a mudança de paradigma acima mencionada na indústria da saúde e do bem-estar.

Trate as toneladas de informações que todos esses sensores portáteis e implantados gerarão, integrando-o com dados de outras fontes, como registros médicos, dados genéticos e até mesmo mídias sociais e usá-lo para desenhar uma imagem ampla do paciente como indivíduo, para para oferecer uma terapia de saúde adaptada - o que a literatura chama de futuro "problema de dados de saúde BIG".

O presente projeto, organizado em torno de 5 (cinco) linhas de pesquisa, incidirá precisamente no desenvolvimento das competências científicas entre os parceiros para enfrentar esses grandes desafios da próxima revolução de saúde e bem-estar.

Uma equipe multidisciplinar de alto nível científico dos parceiros (INESC TEC, IT e CIDESD), interagindo com nossos parceiros associados (grupo IBMC-Microscopia, FMUP-Laboratório de Biologia Experimental e Departamento de Neurocirurgia de FMUP / HSJ) e consultores (Nanium SA - indústria de semicondutores - e empresa de spin-off de tecnologias portáteis da Biodevices SA) será dedicada a abordar os desafios acima mencionados.

CASO REAL DE INSEGURANÇA:

Em 24 de janeiro, Marisa Letícia (mulher de Lula da Silva, ex-presidente do Brasil) passou mal e foi internada no Hospital Sírio-Libanês, em São Paulo. Após a internação, uma médica do Hospital enviou mensagens a um grupo de WhatsApp de antigos colegas de faculdade, confirmando que Marisa Letícia estava nas urgências com diagnóstico de AVC hemorrágico. A mensagem foi compartilhada no grupo "MED IX" e se espalhou em outros grupos de WhatsApp. E um outro médico de fora do Sírio-Libanês postou no grupo imagens de uma tomografia atribuída a Marisa Letícia, acompanhada de detalhes que foram confirmados, em seguida, pela médica. Após esse primeiro vazamento, os arquivos se espalharam nas redes sociais, inclusive com informações que não constavam no boletim divulgado oficialmente pelo hospital, horas depois. Perante esta situação a médica foi demitida e é alvo de sindicância do Cremesp. Uma vez que, segundo o presidente do Conselho Regional de Medicina do Estado de São Paulo (Cremesp), Mauro Aranha: “ a questão do vazamento de exames, prontuarios ou qualquer coisa que revele a doença pela qual a pessoa está passando fere o sigilo médico…” quebrando um dos artigo do código de conduta ética. ~

CONCLUSÕES

A informação médica sobre o paciente individual é considerada altamente privada, e o público em geral é extremamente receoso em relação à divulgação (U.S., 1999). Todos nós apreciamos os benefícios da pesquisa médica realizada em outros pacientes, mas muitas vezes somos relutantes em contribuir ou divulgar nossa própria informação para tais fins. Quando os dados médicos são publicados, espera-se que os pesquisadores mantenham a dignidade do paciente individual e que os resultados serão usados ​​para fins socialmente benéficos (Saul, 2000). Sugeriu-se que as verdades científicas são fundamentalmente amorais; eles podem ser usados ​​para o bem ou o mal (Changeux e Connes, 1995). (d43f81c6e8c3e46f5bdcb686d60d40915de8.pdf)

Prevê-se que, futuramente, os ataques passem a explorar as vulnerabilidades dos softwares associados a equipamentos médicos que se encontrem ligados à rede e interconectados a tecnologias de informação da saúde.

um relatório recente evidencia que equipamentos como bombas de insulina, monitores cardíacos e sistemas PACS têm sido utilizados por ciber-criminosos como um meio de criar uma backdoor e aceder às redes das instituições de cuidados de saúde.