INTRODUÇÃO:

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?

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.

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).

[abordar a necessidade de registos médicos], mas em contrapartida, toda esta informação implica um elevado nível de proteção e segurança devido à sensibilidade da informação clínica e pessoal nela contida.

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.

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.

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

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 informatizados, 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.

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 (tertulia\_1.pdf)

**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).

**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.

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.

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].

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

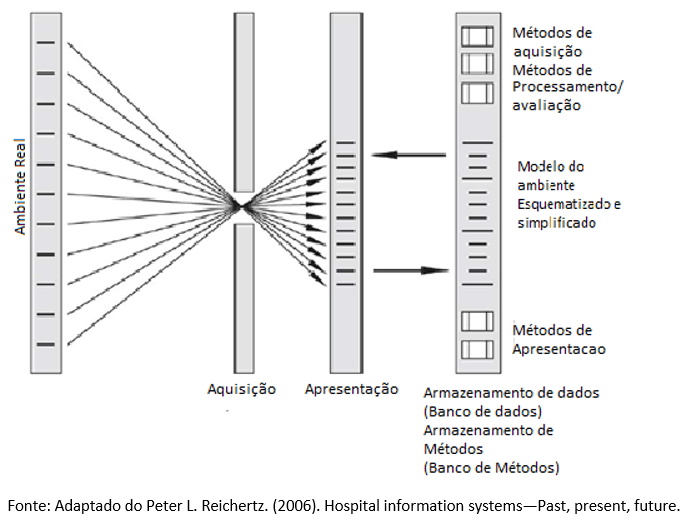
Em certos casos, tem o direito de **exigir que os responsáveis pelo tratamento dos dados corrijam, apaguem ou bloqueiem dados sobre si que estejam incorretos** Trata-se do chamado «direito ao esquecimento».

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:

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).