Em matéria de segurança, o jurista levanta algumas questões: 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?

<https://www.ccip.pt/pt/newsletter-juris/1241-o-novo-regulamento-de-proteccao-de-dados-parte-vii>

---

A estrutura heterogénea dos sistemas de registo clínico electrónico faz com que seja necessário um elevado nível de protecção e segurança devido à sensibilidade da informação pessoal e clínica.

As preocupações de segurança derivam do facto de diferentes fontes terem requisitos tecnológicos diferentes e políticas estabelecidas também diferentes, e do resultado da sua integração poder não ser o esperado. As instituições podem partilhar informação relevante entre si, confiando mutuamente que a informação irá ser mantida confidencial e que será apenas usada para o propósito definido. Neste caso, a linha entre utilizadores internos e externos da rede não está muito bem definida. Pessoas de diferentes organizações podem aceder à informação de muitas outras redes e torna-se difícil gerir e auditar quem tem acesso a que informação e que mecanismos de segurança deverá ter todo o sistema. Por outro lado, como os diferentes módulos têm de ser capazes de interoperar diferentes tecnologias, vulnerabilidades que poderiam ser controladas individualmente poderão ter comportamentos inesperados quando interligados. Outra questão importante, é o uso da linguagem e vocabulário quando se está a desenvolver as interfaces do utilizador. Se as regras não forem consideradas, informação ambígua e redundante poderá ser inserida e mantida o que irá afectar enormemente a eficácia e celeridade do processo de acesso e gestão da informação clínica. Para alem disto, o uso heterogéneo da informação tornará mais difícil a integração de todas as partes que constituem o sistema de registo clínico.

<https://europa.eu/youreurope/citizens/consumers/telecoms-internet/data-protection-privacy/index_pt.htm>

*Actualização : 20/06/2017*

Proteção dos dados e privacidade

Recolha e tratamento dos dados pessoais

Ao abrigo das regras da UE em matéria de proteção de dados, os seus dados pessoais só podem ser tratados em determinadas circunstâncias e condições, nomeadamente:

* se tiver dado o seu consentimento (deve ser sempre informado da recolha dos seus dados)
* se o tratamento dos dados for necessário para celebrar um contrato, candidatar-se a um emprego ou pedir um empréstimo
* se o tratamento dos dados for uma obrigação legal
* se o tratamento for no seu «interesse vital», por exemplo, se tiver tido um acidente e o médico precisar de aceder aos seus dados médicos privados
* se o tratamento for necessário ao exercício de funções de interesse público ou de tarefas a realizar pelas autoridades administrativas, autoridades fiscais, polícia ou outras entidades públicas

Os dados pessoais sobre a sua origem racial ou étnica, orientação sexual, opiniões políticas, religião ou convicções, filiação sindical ou estado de saúde **só podem ser tratados em casos específicos** (por exemplo, se tiver dado explicitamente o seu consentimento ou se, ao abrigo do direito europeu ou do direito nacional, o tratamento for necessário por razões de interesse público).

Estas regras são aplicáveis tanto às entidades públicas como privadas.

## Tratamento dos dados pessoais

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:

* 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 caso de perda, roubo ou utilização ilícita de dados pessoais sensíveis ( **violação de dados pessoais**), o fornecedor de dados deve comunicar esse facto à autoridade nacional para a proteção dos dados[English](http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm). O responsável pelo tratamento dos dados deve também informá-lo se, na sequência de uma tal violação, existirem riscos relativamente aos seus dados pessoais ou à sua privacidade.

## Privacidade nas comunicações eletrónicas (Internet e redes telefónicas móveis)

As regras da UE relativas à proteção dos dados pessoais e da privacidade nas comunicações eletrónicas **abrangem a comunicação por Internet** - como o acesso à Internet - e a comunicação através da **rede telefónica móvel e fixa**.

O seu prestador de serviços deve cumprir as seguintes regras:

* Comunicações confidenciais: sem a sua autorização, não deve ser possível a escuta, a instalação de dispositivos de escuta ou o armazenamento das comunicações.
* Redes e serviços seguros: os prestadores de serviços de comunicações eletrónicas devem adotar medidas para garantir que os seus serviços são seguros.
* Notificação de violações de dados: se um prestador de serviços detetar uma violação da segurança que conduza à **perda ou roubo de dados pessoais**, deve comunicar esse facto às entidades públicas e, nalguns casos, aos assinantes e outras pessoas afetadas.
* Dados de tráfego e de localização: estes **dados devem ser apagados ou tornados anónimos** assim que deixarem de ser necessários para fins de comunicação ou de faturação, a menos que tenha concordado com a sua utilização para outros fins (ou se esta for necessária para efeitos de aplicação da lei).
* «Spam»: **deve dar o seu consentimento** antes de lhe serem enviadas comunicações comerciais não solicitadas (denominadas «spam»), nomeadamente mensagens de texto (SMS) e outras mensagens eletrónicas.
* Listas públicas: deve **dar o seu consentimento prévio** antes do seu número de telefone, endereço eletrónico e endereço postal poderem ser incluídos numa lista pública.
* Identificação de chamadas: deve ter a opção de ocultar o seu número de telefone quando faz uma chamada.

## Direito ao esquecimento

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».

Ale\_Auad\_A importância dos Sistemas de Informacao em Saúde - Estudo de caso USF CelaSaúde Final.pdf

#### A importância dos Sistemas de Informação em Saúde – Estudo de caso na USF CelaSaúde

Os SI podem fazer uso de uma grande diversidade de tecnologias. Quanto ao

aspeto da interface com o utilizador, podem ser aplicações em modo texto, gráficas ou

ambiente Web. A estrutura destes sistemas depende da dimensão da instituição e da

qualidade do sistema. Podem ser:

 Stand-alone - funcionam apenas num computador.

 Cliente-servidor - a aplicação é instalada em vários computadores, mas a

base de dados encontra-se num único servidor.

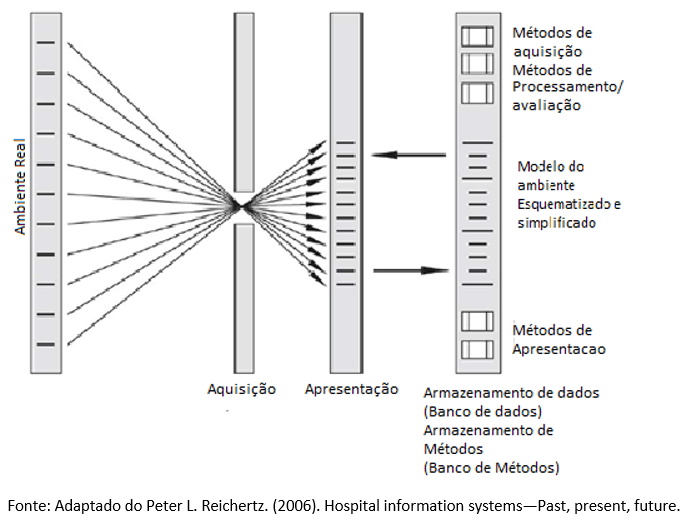
 Em ambiente Web - a aplicação é um conjunto de páginas às quais se pode

aceder de vários computadores, estando assim dados e aplicação no

servidor.

 De acesso remoto - utilizando remote-desktops 1 ou thin-clients 2 para

aceder a ambientes que se encontram no servidor.



CAPÍTULO 4. SISTEMAS DE INFORMAÇÃO UTILIZADOS NA USF CELASAÚDE

DiogoSebe\_SistemaInformacaoEmergenciaMedica.pdf

Plataforma de Dados da Saúde - PDS . . . . . . . . . . . . . . . . . . . 10

APlataformadeDadosdaSaúdeéumsistemawebdepartilhadedados,queexistedesdeMaio de 2012, a nível nacional e permite o registo e partilha de informação clínica. Esta informação pode ser acedida pelos diferentes agentes da prestação de cuidados (utentes, proﬁssionais do SNS edeforadoSNS),atravésdonúmerodeutentedoSNS.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].”

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).

Tecnologias Existentes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

Nassubsecçõesseguintesserãoabordadosaspetosdasegurançaembasededados,assimcomo algumassoluções e tecnologias existentesque ajudama combater oacessoindevidoa informação sensível.

SegurançaemBasedeDados:

A maior preocupação que se coloca num projeto de Tecnologias de Informação é o nível de segurança na proteção de informação conﬁdencial dos utilizadores. Quando se fala em segurança datransferênciadedados,éfrequentequeocontextoemquetaltransferênciaocorresejaemredes pouco seguras e de baixa conﬁança. Existem quatro tipos de ameaças que podem ser exploradas indevidamente [21]:

• 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.