<http://ordemdosmedicos.pt/wp-content/uploads/2017/08/Regulamento_707_2016__Regulamento_Deontol%C3%B3gico.pdf>

pag.5:

Artigo 36.º

Dados médicos informatizados

1 — Os ficheiros automatizados, as bases e bancos de dados médicos, contendo informações extraídas de histórias clínicas sujeitas a segredo médico, devem ser equipados com sistemas, e utilizados com procedimentos de segurança, que impeçam a consulta, alteração ou destruição de dados por pessoa não autorizada a fazê -lo e que permitam detetar desvios de informação.

2 — O acesso aos ficheiros automatizados, as bases e bancos de dados médicos são da responsabilidade de um médico.

3 — Os responsáveis pelos ficheiros automatizados, as bases e bancos de dados médicos, bem como as pessoas que, no exercício das suas fun- ções, tenham conhecimento dos dados pessoais neles registados, ficam obrigados a segredo, mesmo após o termo de funções.

4 — Os ficheiros automatizados, as bases e bancos de dados médicos não podem estar conectados com outro tipo de redes informáticas, a menos que possam garantir -se as condições de segurança referidas no n.º 1.

Artigo 37.º

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.

Artigo 38.º

Responsabilidade do médico com funções diretivas

Os médicos com cargos de direção em organismos prestadores de cuidados de saúde são responsáveis pela adequação às normas deontológicas dos serviços que dirigem, devendo nomeadamente:

a) Estabelecer os mecanismos necessários para a preservação da intimidade e confidencialidade dos doentes;

b) Tratar as informações a serem transmitidas aos meios de comunicação social de um modo adequado e após obtenção do consentimento do doente ou do seu representante legal;

c) Exigir dos seus colaboradores médicos e não -médicos, e ainda dos estudantes das diversas áreas de saúde, a preservação da intimidade e da confidencialidade das informações clínicas, sujeitas a segredo médico.

CAPÍTULO V

Informação médica e Processo clínico

Artigo 39.º

Informação médica

1 — A informação médica é a informação de saúde destinada a ser utilizada em prestações de cuidados ou tratamentos de saúde.

2 — Entende -se por «processo clínico» qualquer registo, informatizado ou não, que contenha informação de saúde sobre doentes ou seus familiares.

3 — Cada processo clínico deve conter toda a informação médica disponível que diga respeito ao doente.

4 — A informação médica é inscrita no processo clínico pelo médico que tenha assistido o doente ou, sob a supervisão daquele, por outro profissional igualmente sujeito ao dever de segredo.

5 — 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.

Pag.6:

Artigo 40.º

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.

Artigo 41.º

Transmissão de dados clínicos entre médicos

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.

Artigo 42.º

Publicações científicas

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.

Artigo 43.º

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.

Artigo 48.º

Garantias de qualidade e segurança

1 — O médico só deve utilizar a telemedicina depois de se certificar que a equipa encarregue da sua realização garante um nível de qualidade suficientemente alto, funciona de forma adequada e cumpre com as normas estipuladas.

2 — O médico deve dispor de sistemas de suporte e utilizar controlos de qualidade e procedimentos de avaliação para vigiar a precisão e a qualidade da informação recebida e transmitida.

3 — O médico só deve utilizar a telemedicina depois de se certificar que o sistema utilizado e os seus utilizadores garantem o segredo mé- dico, nomeadamente através da encriptação de nomes e outros dados identificadores.

Pag.7:

Artigo 49.º

História clínica

1 — O médico que utilize a telemedicina deve registar na ficha clínica os métodos de identificação do doente, as informações pretendidas e as recebidas.

2 — O médico teleconsultado deve registar em ficha clínica as opiniões que emitiu e também a informação em que se baseou.

3 — Os métodos informatizados de arquivamento e transmissão dos dados do doente só devem ser utilizados quando se tenham tomado medidas suficientes para proteger a confidencialidade e a segurança da informação registada ou permutada.

<http://ordemdosmedicos.pt/wp-content/uploads/2017/09/Protocolo_IMED.pdf>

ACORDO Ordem dos Médicos / iMED

Artigo 1

Plataforma iMED e Enquadramento

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.

Artigo 2

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.

Artigo 3

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.

Site:

<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.

VANTAGENS

* Tecnologia totalmente web, alojada na Cloud;
* Não precisa instalar ou efetuar configurações no seu computador;
* Dispõe de aplicação móvel para iOS e Android;
* Tempo de atendimento inferior a 10 segundos;
* 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;
* Atualizações tecnológicas e legislativas gratuitas.

SERVIÇOS (mais: <https://www.imed.pt/imed/index.php?mod=conf&op=login_form&opt=produto> )

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.

Cloud:

<http://www.acin.pt/>

<http://ordemdosmedicos.pt/wp-content/uploads/2017/09/Protocolo_MedicineOne.pdf>

PROTOCOLO DE COOPERAÇÃO ENTRE MedicineOne E A ORDEM DOS MÉDICOS

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.

A Ordem dos Médicos tem tido a preocupação de que, seja a nível do SNS, seja a nível da prestação privada de cuidados de saúde, os Médicos possam dispor de ferramentas informáticas que, com o menor custo, lhes permitam estar em conformidade com a Lei.

Considerando que:

1. O My MedicineOne é uma aplicação de gestão clínica.
2. A Ordem dos Médicos é uma 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,

CLÁUSULA 1ª

Objetivos gerais

O presente Protocolo tem como objetivo principal: a) contribuir para alargar o leque de opções de ferramentas informáticas que permitam, no cumprimento da Lei, a prescrição electrónica, através da disponibilização do programa My MedicineOne.

CLÁUSULA

2ª Objetivos específicos

permitir à Ordem dos Médicos, durante a vigência do Protocolo, sugerir aos seus associados uma solução gratuita de qualidade reconhecida, que inclui as seguintes funcionalidades, que vão além do legalmente exigido, nomeadamente:

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.

Site:

<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...

Ver:

<https://kb.medicineone.net/m8_medicineone/#.medicineone>

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

**RNU – Registo Nacional de Utentes**  
O Registo Nacional de Utentes é um dos pilares do sistema de informação da saúde (SIS). 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.  
No âmbito do CC, 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.

<https://www.dn.pt/sociedade/interior/ordem-dos-medicos-pede-parecer-sobre-partilha-de-dados-dos-doentes-8809630.html>

30 DE SETEMBRO DE 201709:38

Em causa está uma alteração na aplicação informática dos médicos de família que passa a obrigar os clínicos a pedir aos doentes consentimento informado para partilha, numa plataforma eletrónica, dos resultados dos meios complementares de diagnóstico realizados na medicina convencionada.

 o bastonário adianta que vai enviar aos SPMS duas "sugestões essenciais".

"O médico tem de poder recusar pedir o consentimento e o sistema informático deve contemplar essa possibilidade", referiu Miguel Guimarães, adiantando ainda que deve ser salvaguardado o privilégio terapêutico.

A Ordem pretende ainda que fique "claramente escrito e expresso no texto da plataforma" que não é dos médicos a responsabilidade da utilização dos dados clínicos, a partir do momento em que são partilhados numa plataforma eletrónica.

Segundo a carta enviada à Ordem, quando o médico vai pedir um exame, surgem na aplicação informática duas frases, sendo que cabe ao clínico assinalar uma delas.

"O utente declarou expressamente consentir que os resultados dos exames realizados sejam disponibilizados na sua área do cidadão, podendo ser consultados pelos profissionais de saúde do Serviço Nacional de Saúde", é a frase que surge assinalada por defeito.

A outra opção refere: "O utente declarou expressamente não consentir que os resultados dos exames realizados sejam disponibilizados na sua área do cidadão".

Na carta dirigida à Ordem, a médica de família refere que não há "qualquer condição para, em todas as consultas com pedido de meios complementares de diagnóstico, os médicos de família estarem a informar os pacientes da arquitetura de confidencialidade dos sistemas informáticos do SNS".

Acrescenta a médica que esta "não é uma função" que compita aos médicos, considerando que "este é mais um exemplos das incontáveis e permanentes ingerências na atividade clínica e nos registos dos médicos de família".

Além disso, na carta, a médica sublinha que o Ministério da Saúde partilha há anos na plataforma de dados da saúde (PDS) e "sem qualquer aviso prévio" a informação clínica dos utentes constante dos processos eletrónicos.

"Lembro que há anos acedem à PDS indiscriminadamente médicos, enfermeiros, assistentes sociais, psicólogos e nutricionistas de qualquer estabelecimento do SNS", podendo aceder a registos de exames, de medicação ou de consultas, refere a mesma médica na carta que o Sindicato Independente dos Médicos (SIM) decidiu tornar pública através do seu 'site'.

Em declarações à agência Lusa, o secretário-geral do SIM, Roque da Cunha, considerou que esta tarefa de pedir o consentimento aos doentes e de explicar a partilha de dados "não compete aos médicos de família" e que irá "tornar mais pesado o acompanhamento de 1.900 utentes por cada médico".

<https://www.publico.pt/2017/09/30/sociedade/noticia/ordem-dos-medicos-pede-parecer-sobre-partilha-de-dados-dos-doentes-1787248>

30 de Setembro de 2017, 11:24

**Dados dos doentes demasiado acessíveis**

Além das questões relacionadas com a partilha na plataforma electrónica, a Ordem dos Médicos avisa que os dados dos doentes estão demasiado acessíveis nos hospitais a diferentes profissionais e considera que os actuais sistemas informáticos protegem pouco os dados pessoais.

"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", afirmou à agência Lusa o bastonário da Ordem dos Médicos.

Para o bastonário, são actualmente muito poucos os dados dos doentes que têm uma protecção que possa ser considerada adicional. "Isto é um problema actual. Mas quem é responsável pela partilha dessa informação de doentes não são os médicos", comentou Miguel Guimarães.

Aliás, o bastonário discorda que tenha de caber aos médicos pedir aos doentes consentimento para partilhar informações do doente quando o médico não controla para onde vai essa informação.

"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", considerou.

VER:

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

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

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

<https://www.sns.gov.pt/home/apps-da-saude/>

<http://www.cert.pt>

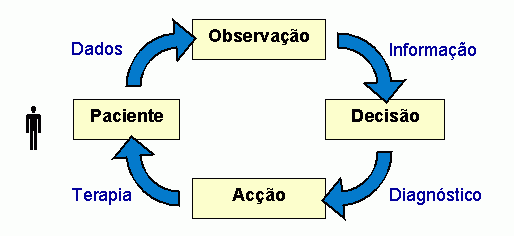
<http://spms.min-saude.pt/product/area-cidadao/>

<http://spms.min-saude.pt/2013/11/pds-plataforma-de-dados-da-saude/>

trabalho:

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

O processo clínico propriamente dito envolve uma série de etapas como observação, decisão e plano de acção. Só se pode perceber a organização do processo clínico em geral, e do processo clínico em papel ou electrónico, em particular se se conhecer os vários tipos de informação que se dispõe para se tomar uma decisão clínica.   
Numa primeira fase, a partir da observação de dados recolhidos do paciente, que incluem dados narrativos, como a história clínica ou a opinião do médico, medidas numéricas, como dados do exame físico (temperatura, tensão arterial, idade, etc) é gerada informação.  
Depois com base no conhecimento do clínico, existe uma interpretação desta informação que dá origem a hipóteses de diagnóstico. Em presença do diagnóstico (doença) é iniciada uma acção terapêutica.



É com base nesta informação que é organizado o processo clínico. Este contém toda a informação relativa à saúde e à doença de um paciente desde o momento que ele contactou o profissional de saúde.

A informação existente num registo clinico corresponde a informação maioritariamente alfanumérica, ou seja, que pode ser representada por **caractéres**ou **dígitos**. A restante informação não textual, 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.

Neste tipo de registo podemos normalmente distinguir na sua organização dados de:

* carácter administrativo:
  + nome
  + data de nascimento
  + a identificação do doente
* dados médicos fixos (ocorrências singulares):
  + sexo
  + grupo sanguíneo
  + alergias
* outros dados médicos (ocorrências múltiplas de dados ou dados temporais):
  + história clinica
  + exame obectivo
  + diagnósticos
  + procedimentos
  + terapêutica
  + ...

A organização do processo clínico depende das preferências do clínico e das orientações do local onde trabalha.

--

O registo clínico em papel é uma forma de registo clínico, tal como está descrita no capítulo anterior, em que os dados clínicos são introduzidos de forma manuscrita, e toda a informação clínica é anexada a este processo em papel.

Como se pode compreender a partir da organização do processo clínico, os dados clínicos de um paciente tem origens muito diversas, desde história clínica e exame objectivo até resultados de exames auxiliares de diagnóstico.   
O registo clínico é um sistema de armazenamento de informação clínica, 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/papel.gif | http://im.med.up.pt/epr/esquema_papel.gif |

Como se pode ver pela figura o registo clínico em papel corresponde à centralização de todo a informação clínica do doente, não permitindo *feed-back*desta informação.

A estruturação da informação clínica introduzida no processo em papel depende do médico ou da organização do serviço ou departamento. É possível que os dados clínicos não tenham qualquer estruturação. Tal como é habitual os dados são organizados de forma cronológica. Por este motivo a forma de acesso **à informação está limitada.**

**Outros inconvenientes são:**

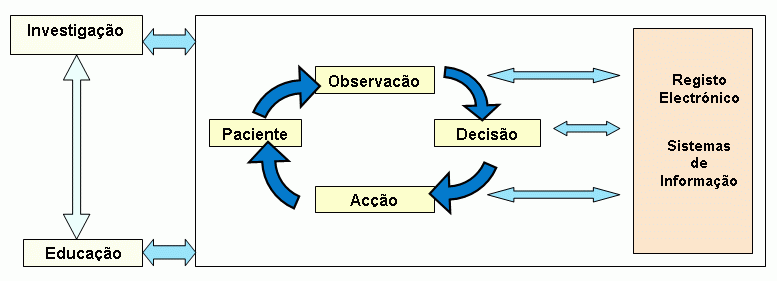
* Ilegibilidade dos registos médicos por outros profissionais de saúde
* Inconsistência de formato e de localização da informação
* Falta de estruturação interna dos registos
* Perda de informação
* Duplicidade de informação.

**Por outros lado os registos em papel têm algumas vantagens:**

|  |
| --- |
| * São facilmente transportáveis * A introdução de dados está facilitada * Cada profissional adapta o registo às suas preferências * Versatilidade no registo de dados * Não obrigam a formação específica |

Uma das aplicações mais directas da informática à medicina, prende-se com a criação dos registos clínicos electrónicos, na tentativa de substituir os registos clínicos em papel. É importante referir que os registos clínicos electrónicos vão muito além da informatização dos registos em papel. Estes sistemas permitem:

* auxiliar na prestação de cuidados de saúde
* auxiliar a decisão clínica
* avaliar a qualidade dos cuidados prestados
* fazer a gestão e planeamento dos recursos de saúde
* auxiliar na investigação
* auxiliar na educação médica



Relação das várias etapas da actividade médica com os sistemas de informação e relação com outras áreas.

### *Cinco níveis de registos clínicos electrónicos*

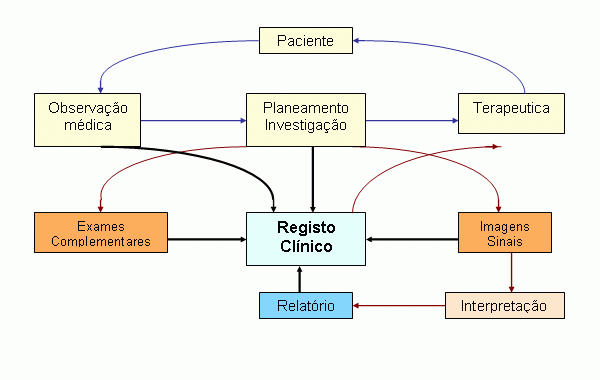
Baseado no trabalho de Peter Waegmann, MRI, 1997.

1. **Registo Clínico Automatizado**: funciona em paralelo com o registo em papel; passos incrementais para a informatização; inicio de reengenharia.
2. **Registo Clínico Computadorizado**: imagem do documento; documentação tradicional mas sem papel; aumento da reengenharia.
3. **Registo Clínico Electrónico**: os profissionais interagem com o computador; diferentes fontes de informação; reengenharia completa com funcionalidade adicionais.
4. **Registo Electrónico do Paciente**: informação de saúde e interoperabilidade; regional / nacional / global; consenso em relação a confidencialidade / segurança.
5. **Registo Electrónico de Saúde**: envolvimento do utente; bem-estar integrado; informação de saúde não tradicional.

Um registo 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).



Um registo clínico para além de poder conter toda a informação clínica relatica a um paciente, independentemente da origem, também pode permitir a visualização dos dados clínicos, sob várias formas, pode partilhar informação entre vários utilizadores, pode restringir o acesso aos dados clínicos ou mesmo disponibilizar formas de analisar a informação.

Nos cuidados de saúde devem ser considerados 2**níveis de prestação de cuidados**que têm necessidades diversas:

* **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.

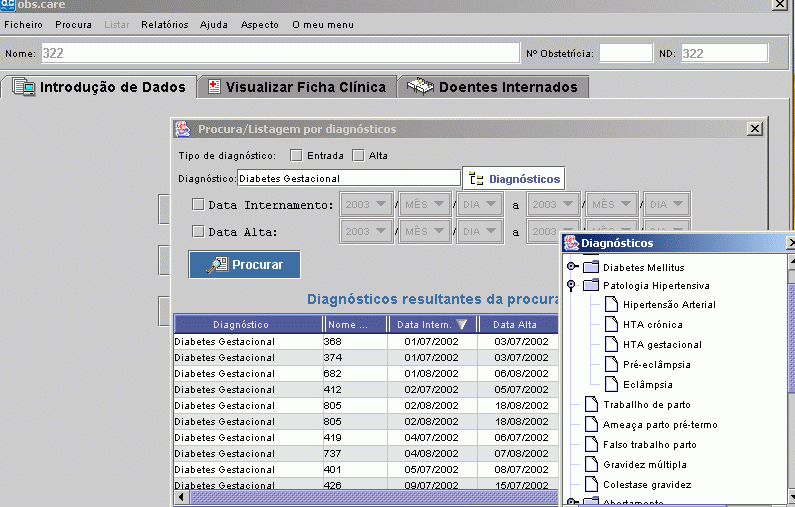
<http://epr.med.up.pt/intensive/index.html>

**Acesso aos dados**

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

Exemplo de pesquisa por diagnóstico

Algumas vantagens na implementação de registos electrónicos do doente:

* Facilidade no acesso à informação (ex.: permitem o acesso simultâneo a partir de diferentes localizações)
* Legibilidade
* Maior velocidade no acesso à informação
* Melhor protecção da informação que no sistema em papel
* Informação actualizada
* Permite ter um processo clínico com toda a informação clínica do doente
* Precisão na informação (ex.: suporte para a entrada de dados estruturada)
* Variedade na formas de visualizar os dados
* Apoio à decisão
* Possibilidade de análise de dados
* Possibilidade de troca de informação clínica, entre cuidados primários e de especialidade, permitindo o aparecimento de cuidados de saúde partilhados
* Regulamentos mais respeitados

Alguns problemas na implementação de registos electrónicos:

* Introdução de dados inicialmente mais lenta
* Necessitam de formação específica dos profissionais de saúde
* Consumo de recursos iniciais na educação e treino
* Obriga a actualização de conhecimentos constante
* Pouca flexibilidade nas restrições impostas ao acesso da informação (se a pessoa que tem acesso não está disponível o acesso não se realiza)
* Não dão muita liberdade no estilo de escrita dos relatórios
* O registo pode-se perder se os procedimentos correctos não forem executados
* Não podem ser transportados facilmente de um lado para outro
* Por vezes os sistemas não estão disponíveis, algo que não acontece nos registos em papel
* Problemas de quebra de segurança

<http://im.med.up.pt/seguranca/index.html>

### *Evolução das tecnologias*

A quantidade de dados armazenada em bases de dados, bem como o acesso a estes dados, tem vindo a aumentar face à generalização das redes de computadores não só dentro de cada instituição ([LAN](http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=LAN)) mas também entre diferentes instituições da saúde ([MAN](http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=MAN) / [WAN](http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=WAN)). Isto é ainda mais notório com a introdução de novas tecnologias, como as redes sem fios ([WLAN](http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=WLAN)), onde o acesso à Internet e a bases de dados online é cada vez mais independente do local físico.

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).

**Alguns aspectos menos positivos a considerar quando são utilizados sistemas de informação**:

1. A maior acessibilidade aos dados pode ser uma ameaça para a privacidade daqueles cujos dados estão disponíveis electronicamente - devem ser adoptadas medidas para prevenir a ocorrência de acessos não autorizados **[confidencialidade]**;

2. Erros nos dados e no software podem acontecer e devem ser mantidos dentro de limites aceitáveis, proporcionando a qualidade e validade dos mesmos - a protecção contra a perda ou corrupção dos dados é um dos aspectos a considerar **[integridade]**;

3. Cada vez mais as instituições de saúde estão dependentes do funcionamento dos seus sistemas de informação a todo o momento, o que implica a necessidade de cada vez mais acções com o intuito de diminuir a probabilidade de interrupções nos serviços - devem ser adoptadas medidas para que o acesso autorizado a informação confidencial esteja disponível sempre que necessário**[disponibilidade]**.

As medidas a adoptar para protecção dos dados podem dizer respeito aos equipamentos, às pessoas, ao software e aos procedimentos. É impossível garantir uma segurança a 100%, no entanto é possível reduzir os riscos ou restringir possíveis danos devido à má utilização ou ao uso abusivo.

## *Ética vs Privacidade*

Todas as interacções sociais estão sujeitas a vários princípios fundamentais da Ética. Os profissionais de Saúde trabalham num ambiente social e, como tal, as suas acções são também sujeitas a esses princípios.

Alguns destes princípios são: o Príncipio da Autonomia, o Príncipio da Igualdade e Justiça, o Príncipio da Beneficência, o Princípio da Integridade, etc.

Estes Príncipios Éticos, quando aplicados a situações no domínio da Informática, dão origem aos Príncipios Éticos da Informática:

**Princípio da Privacidade**, **Princípio da Transparência**, **Princípio da Segurança**, **Princípio do Acesso**, etc.

Os Princípios mais estreitamente ligados com a segurança da informação são:

o **Princípio da Privacidade**: Todas as pessoas têm o direito fundamental à privacidade e, por conseguinte, ao controlo sobre a recolha, armazenamento, acesso, uso e transmissão dos seus dados pessoais;

o **Princípio da Segurança**: os dados que tenham sido recolhidos sobre determinado indivíduo devem ser protegidos contra a perda, corrupção, destruição, acesso, uso e alteração indevidas ou não autorizadas;

## *Privacidade vs Confidencialidade*

Os 2 Princípios acima introduzem conceitos muito importantes como é a privacidade dos dados.

A**privacidade**é muitas vezes confundida com o termo **confidencialidade** e, até, com a própria segurança em geral.

**Privacidade** diz respeito ao direito fundamental de cada **indivíduo** de decidir quem deve ter acesso aos seus dados pessoais;

**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.

A confidencialidade é então uma das principais características da segurança.

## *Características da Segurança*

### Confidencialidade

Confidencialidade consiste em previnir o acesso não autorizado a informação confidencial.

Esta característica confunde-se muitas vezes com o termo privacidade mas não significa o mesmo. Privacidade é uma das razões para haver segurança, e mais especificamente, confidencialidade. Se determinada informação é considerada privada por quem a detém ou tem direitos sobre ela, é neste âmbito que é definido quem ou o quê tem acesso a essa informação. Confidencialidade consiste em que essas regras sejam postas em prática (como definido acima), mantendo confidencial a informação privada.   
Assim, o direito de acesso à informação dependerá de vários factores tais como:

o A legislação corrente  
o A opinião pública  
o A política institucional  
o Qual a importância dessa informação para o negócio/natureza da Instituição  
o A atitude das instituições  
o A quem pertence a informação  
o Política e direitos dos utilizadores (se fizer sentido)

### ***Integridade***

Integridade consiste em previnir a alteração ou modificação não autorizada de informação confidencial.

A obtenção deste objectivo passa pela:

o Definição de quem ou o quê tem direitos para realizar alterações  
o Documentação: especificações técnicas e manuais de utilização  
o Verificação: determinação da conformidade do sistema com as suas especificações funcionais  
o Validação: avaliação do grau de sucesso na realização dos objectivos e efeitos propostos

### Disponibilidade

Disponibilidade consiste no acesso autorizado a informação confidencial sempre que necessário.

A informação apenas é importante e útil se puder ser disponibilizada no momento em que dela se necessita.

São consideradas ameaças à segurança, as ameaças a qualquer umas das suas três características essenciais:

### ***Ameaças à confidencialidade***

A confidencialidade é violada quando os dados passam para mãos erradas (não autorizadas), quer seja de propósito, quer acidentalmente, dentro ou fora da Instituição.

**Exemplos de problemas são:**

o problemas de acesso não autorizado;  
o vulnerabilidades do login/password (e.g. partilha de passwords);  
o intercepção não autorizada da informação em trânsito (e.g. sniffing);  
o gestão não controlada da informação;

### Ameaças à integridade

A integridade está ameaçada quando, propositada ou acidentalmente, houver inconsistência nos repositórios de dados ou quando os seus conteúdos estiverem, por algum motivo, corrompidos.

**Exemplos de problemas são:**

o Erros no software;  
o Mau funcionamento de equipamento;  
o Erros operacionais (e.g. na introdução de dados);  
o Vírus que corrompem a informação;

### ***Ameaças à disponibilidade***

A disponibilidade da informação é uma característica muitas vezes esquecida, mas cada vez mais essencial. As ameaças à disponibilidade dos dados ou às funcionalidades do sistema ocorrem quando é impossível ao sistema completar, no momento que lhe é pedido, tarefas que normalmente lhe são exigidas.

**Exemplos de problemas são:**

o Falhas nos equipamentos ou serviços de rede (e.g. ao nível do hardware/software, falhas de energia, erros/bugs);  
o Erros no manuseamento do sistema;  
o Causas naturais (incêndios, inundações);  
o Recursos insuficientes para o correcto funcionamento do software;  
o Quando ocorrem ataques propositados para impedir o funcionamento normal do sistema (e.g DOS-Denial of Service attacks, SPAM);

### Detecção e Correcção

Minimizar os estragos quando alguma coisa corre mal. Por exemplo: minimizar o tempo de indisponibilidade do sistema, recuperação de informação com cópias de segurança.

|  |  |  |
| --- | --- | --- |
|  | **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 |

### Mecanismos de Segurança

**Confidencialidade**: Controlo de acesso (incluindo identificação única de utilizadores, utilização de um serviço de directórios para armazenamento de informação sobre os utilizadores do sistema, aplicação de uma pré-norma Europeia [CEN/TC251 - ENV 12251 (1999): Health Informatics]); Segurança nas comunicações (utilização de criptografia com a aplicação de um protocolo para encriptação de informação em trânsito).  
**Integridade**: Assinaturas Digitais dos relatórios (utilização de um algoritmo open source, baseado numa norma, para encriptar e assinar digitalmente os relatórios antes do seu armazenamento: permite a verificação da integridade aquando do acesso a um relatório).  
**Disponibilidade**: Redundância de Equipamento (hardware/software); Backups (feitos regularmente e armazenados em locais separados da utilização do sistema); Auditoria (identificação única de utilizadores;   
criação de sessões por utilizador; monitorização e armazenamento de informação relativa a acessos à informação, erros de sistema e outros problemas de uso).

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

Em declarações, Henrique Martins, presidente dos Serviços Partilhados do Ministério da Saúde (SPMS), cuja 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.atlasdasaude.pt/publico/content/justica-e-saude-vao-partilhar-dados-clinicos-de-reclusos-e-utilizar-telemedicina>

<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".