

RELATÓRIO DE AUDITORIA
AO TRATAMENTO DE
INFORMAÇÃO DE SAÚDE NOS
HOSPITAIS

RELATOR – AMADEU GUERRA
APROVADO NA SESSÃO PLENÁRIA DE 9 DE NOVEMBRO DO 2004

INDICE

	Pág.
I – Introdução. Objectivos delineados	3
II – Tratamento da Informação	
1. Obrigação de notificação e controlo prévio pela CNPD	5
2. Direito de Informação e acesso	7
3. Respeito pelo princípio da finalidade	15
4. Utilização de dados de saúde para investigação científica	16
5. Confidencialidade e regras de segurança	20
6. Prazo de conservação e informação de saúde	29
III – Considerações Gerais sobre o Tratamento de Informação de Saúde nos Hospitais	
1. Rede hospitalar e gestão da informação de saúde	30
2. A utilização dos sistemas de videovigilância	39
IV – Aspectos Particulares Verificados	
1. As experiências de telemedicina	41
2. Os pedidos de análises clínicas e o acesso aos resultados:	46
2.1. Antecedentes	46
2.2. A situação actual	48
2.3 Solução preconizada para reforçar a confidencialidade	54
3. Arquivo clínico	56
4. Caminhar para um <i>dossier</i> clínico informatizado	65
CONCLUSÕES	70
RECOMENDAÇÕES	74
ANEXOS	78

I. INTRODUÇÃO. OBJECTIVOS DELINEADOS

O Plano da Actividades da Comissão Nacional de Protecção de Dados (CNPD) prevê, para o ano de 2004, a realização de uma *«fiscalização de controlo a instituições de saúde»* que consiste no *«levantamento da situação dos tratamentos de dados pessoais em diversas instituições de saúde públicas e privadas de regiões diversas»*.

Para levar a cabo esta tarefa a CNPD fez uma visita a 38 hospitais (*Anexo I*) com o objectivo de verificar a forma como se procedia ao tratamento de dados de saúde dos doentes. Na Região Autónoma da Madeira alguma da informação coligida pelo Centro Hospitalar do Funchal pode ser partilhada pelos Centros de Saúde. Na Região Autónoma dos Açores foram visitados 2 Centros de Saúde que, por terem características específicas (v.g. realização de internamentos e urgência), foram também objecto de análise.

A CNPD não verificou quaisquer outros tratamentos de dados existentes nos hospitais que não se relacionassem com a realização de finalidades relativas a medicina preventiva, de diagnóstico médico ou de prestação de cuidados de saúde. Para além do tratamento de informação em «bases de dados», foram ainda considerados os tratamentos de dados em suporte de papel e as experiências de «telemedicina».

Não foram objecto de análise, nomeadamente, as aplicações relativas ao processamento de remunerações, à gestão administrativa de funcionários, ao controlo dos trabalhadores em matéria de utilização do correio electrónico ou Internet⁽¹⁾, bem como outras aplicações de gestão administrativa e financeira.

Verificando-se uma tendência generalizada para a adopção de sistemas de videovigilância nos Hospitais a CNPD fez, igualmente, o levantamento destes tratamentos.

⁽¹⁾ Em muitos hospitais foi abordada esta temática e perguntado se existia uma política de controlo dos trabalhadores. A CNPD informou sobre a existência de orientações relativas ao controlo de trabalhadores (disponíveis in <http://www.cnpd.pt>), tendo tomado medidas, num caso concreto, de proibição de publicitação na rede do Hospital das consultas realizadas a sítios Internet por posto de trabalho.

A acção desenvolvida visa, exclusivamente, verificar se o tratamento de dados de saúde respeita as condições legalmente estabelecidas pela Lei 67/98, de 26 de Outubro, e se são respeitados os direitos dos doentes consignados, nomeadamente, na Lei de Bases da Saúde (Lei n.º 47/90, de 24 de Agosto). De entre outras, houve preocupações particulares em relação à análise dos seguintes aspectos:

- a) Se a recolha de dados e tratamento subsequente era feito com observância do princípio da transparência (artigo 2.º da Lei 67/98) e com salvaguarda do direito de informação dos doentes (artigo 10.º da Lei 67/98);
- b) Se os dados pessoais dos doentes eram tratados no âmbito de finalidades determinadas e legítimas (a prevenção, diagnóstico, prestação de cuidados e gestão de serviços de saúde), se havia tratamento subsequente compatível com esta finalidade (v.g. investigação científica) e se esse complexo de tratamentos cumpriam as «condições de legitimidade» legalmente previstos no artigo 7.º da Lei 67/98;
- c) Se os tratamentos respeitavam, em todas as suas vertentes, o segredo médico e o «estatuto dos utentes» que se consubstancia no direito de ser «respeitada a confidencialidade sobre os dados pessoais revelados» (cf. Base XIV n.º 1 al. d) da Lei de Bases da Saúde aprovada pela Lei n.º 47/90, de 24 de Agosto). Para além das medidas adoptadas com vista a evitar o acesso/divulgação de dados a terceiros estranhos à instituição hospitalar, houve uma preocupação de verificar que tipo de procedimentos ou medidas são adoptadas para impedir o acesso – no seio da instituição hospitalar – a dados de saúde por pessoas não autorizadas legalmente.
- d) O direito de acesso aos dados pelo próprio doente (cf. artigo 11.º n.º 5 da Lei 67/98) deverá ser, igualmente, objecto de reflexão.

A CNPD propõe-se fazer um levantamento tão completo quanto possível da forma como são tratados os dados de saúde, evidenciando os aspectos positivos e procurando, em relação a alguns procedimentos menos adequados, sugerir alterações organizativas ou procedimentais e, em situações específicas, propor medidas legislativas adequadas.

II. O TRATAMENTO DA INFORMAÇÃO E O CUMPRIMENTO DA LEI 67/98, DE 26 DE OUTUBRO

1. A obrigação de notificação e o controlo prévio pela CNPD

1. O artigo 27.º n.º 1 da Lei 67/98, de 26 de Outubro, estabelece a obrigatoriedade de notificação «antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados, destinados à prossecução de uma ou mais finalidades interligadas».

Quando está em causa o tratamento de dados pessoais realizados nas circunstâncias estabelecidas no artigo 7.º n.º 2 da Lei 67/98, a realização do tratamento carece de «**autorização prévia da CNPD**».

A CNPD tem entendido que o tratamento de dados referentes à saúde, à vida sexual ou dados genéticos, realizados para a finalidade e nas circunstâncias estabelecidas no artigo 7.º n.º 4 não estará sujeito a controlo prévio. Porém, se houver tratamento de outros dados (v.g. raça, fé religiosa ou outros dados da vida privada – toxicod dependência, comportamento de risco, hábitos alcoólicos, problemas sociais de integração), os dados de saúde, da vida sexual ou genéticos forem utilizados para finalidades diversas (v.g para fins de investigação científica) ou tratados em circunstâncias diversas das estabelecidas no artigo 7.º n.º 4 (tratamento efectuado por pessoa não obrigada a sigilo profissional ou sem garantia da medidas de segurança), devem os responsáveis submeter tais tratamento a **controlo prévio/autorização** da CNPD.

2. De entre os 38 hospitais visitados havia 6 que não tinham feito, à data da visita da CNPD, a notificação de qualquer tratamento. Em relação aos hospitais que realizaram notificação de tratamentos (32), consta do registo da CNPD a notificação de 195 tratamentos⁽²⁾.

Não sendo o objectivo da CNPD fazer um levantamento exaustivo da totalidade dos tratamentos existentes nos hospitais visitados, foi possível encontrar – por visita aleatória a determinados serviços – que havia muitos *tratamentos não notificados*, apresentando-se de seguida um quadro relativo à notificação de tratamentos:

Finalidades	Notificados	Não notificados
Análises/Serv. Sangue	14	49
Arquivo	24	16⁽³⁾
Telemedicina	0	54
Videovigilância	4	17
Outras Finalidades ⁽⁴⁾	153	57
Total	195	193

Verificados os termos das notificações realizadas com as aplicações instaladas podemos afirmar que, em termos gerais, os tratamentos estão a ser feitos em conformidade com as respectivas notificações. Existem situações pontuais em que foi omitido o tratamento de alguns dados (v.g. dados sensíveis – raça, toxicodependência, prostituição), tendo também havido uma falta de cuidado generalizada na especificação das condições em que os dados são subsequentemente utilizados para fins de investigação.

⁽²⁾ De entre estes há 6 hospitais que fizeram a notificação de mais de 10 tratamentos.

⁽³⁾ 10 destes tratamentos não notificados dizem respeito à aplicação “SONHO”, a qual foi comunicada pelo IGIF. Isto é, não consta dos processos de notificação destes Hospitais qualquer referência à aplicação em causa.

⁽⁴⁾ Engloba a generalidade dos tratamentos nos diversos serviços ou especialidades (v.g. gestão de doentes, cardiologia, obstetrícia, ginecologia, oncologia, Urgência, UCI, infectocontagiosas, etc.)

Em relação à omissão da obrigação de notificação pode concluir-se que, estando a generalidade dos hospitais conscientes de que devem fazer as respectivas notificações, não houve da sua parte a preocupação de fazer um levantamento exaustivo dos tratamentos em curso em todo o hospital. Não se compreende como é possível continuar a encontrar uma percentagem elevada de tratamentos não notificados (cerca de 50%) por parte da generalidade dos hospitais. Como se verá, deve ser dada particular atenção às aplicações da responsabilidade exclusiva de médicos por poderem representar, em termos gerais, um maior perigo em termos de privacidade dos doentes (v.g. por não estarem dotadas de *password* ou não fazerem a separação lógica dos dados) ou por envolverem um risco em relação à integridade dos dados (por não serem feitas cópias de segurança ou não haver suportes alternativos para preservar a perda accidental dos dados).

A manter-se esta situação a CNPD irá desenvolver acções de fiscalização, com vista à aplicação das respectivas sanções legalmente previstas (coimas ou participação criminal ao Ministério Público, conforme as circunstâncias). Irão merecer cuidado especial os tratamentos sujeitos a *controlo prévio* pela especial sensibilidade dos dados tratados e pelo risco de discriminação dos seus titulares⁽⁵⁾.

2. Direito de informação e acesso

1. Nos termos do artigo 10.º da Lei 67/98 o responsável está obrigado a assegurar o ***direito de informação***, em particular sobre a identidade do responsável, finalidade do tratamento, destinatários ou categorias de destinatários dos dados e formas e condições do exercício do direito de acesso e rectificação por parte dos titulares dos dados.

⁽⁵⁾ Vejam-se, para maior detalhe, as considerações tecidas em relação aos serviços de sangue e à utilização de dados para fins de investigação científica.

Em nenhum Hospital – à excepção daqueles onde havia avisos afixados a informar sobre a recolha de imagens no âmbito da videovigilância (cf. adiante) – foram adoptados mecanismos concretos que se destinem a assegurar o *direito de informação*. Ou seja, não foram encontrados formulários, avisos ou quaisquer procedimentos que se destinassem a dar o direito de informação nas vertentes acima enunciadas.

Em dois hospitais foi dito que era obtido o «consentimento informado» dos utentes. No entanto, e compulsados os respectivos suportes de papel foi possível verificar o seguinte:

- 1) Num dos casos o «*consentimento informado*» – procedimento de recolha estabelecido através de disposições escritas e que vinculam todos os Departamentos ou Serviços de Acção Médica do Hospital – *só é aplicável no domínio da realização de actos médicos* («procedimentos médicos ou cirúrgicos») que devem ser especificados e clarificados ao doente⁽⁶⁾. Em nenhuma disposição escrita dos «procedimentos» se especifica que tal consentimento se reporta ao tratamento de dados pessoais do doente. A declaração de consentimento⁽⁷⁾, reportando-se apenas à necessidade de «descrição do procedimento médico, cirúrgico ou anestésico», não apresenta qualquer referência aos elementos constantes do artigo 10.º n.º 1 da Lei 67/98.
- 2) Noutro caso a «declaração» é obtida no âmbito do inquérito detalhado feito pelo Serviço de Imuno-Hemoterapia no momento prévio à selecção dos dadores de sangue. O texto incluído no formulário tem a seguinte redacção: *“tenho conhecimento de que serão feitas análises no meu sangue requeridas pela lei e aceito que o meu nome faça parte de uma lista que pode ser consultada por todos os Serviços de Sangue dos Hospitais e o Instituto Português de Sangue, no caso de algum resultado ser positivo. Nestas circunstâncias, autorizo que me seja feita uma colheita de sangue e assino voluntariamente esta declaração, em plena consciência das minhas responsabilidades”*.

⁽⁶⁾ De acordo com as respectivas regras escritas sobre este procedimento, «aos doentes, utentes ou seus representantes legais devem ser prestados todos os esclarecimentos por eles solicitados, de modo a que lhes permita atingirem o alcance do(s) procedimento(s) que lhes é(são) proposto(s), explicando os procedimentos alternativos, de forma a que, em consciência, se sintam habilitados a decidir».

⁽⁷⁾ O «consentimento informado» deve ser obtido pelo médico e será sempre arquivado no processo clínico do doente.

Tal como resulta da declaração, o consentimento limita-se a autorizar a disponibilização do nome do titular aos Serviços de Sangue e IPS em relação a situações em que haja resultados positivos que determinem (transitória ou definitivamente) a impossibilidade de dar sangue. Constatou-se que estes serviços recolhem muitos outros dados – alguns deles extremamente sensíveis (hábitos sexuais, parceiros, diagnóstico de doenças sexualmente transmissíveis, prostituição, consumo de álcool e de drogas, HIV) – e não é feita qualquer referência ao seu tratamento automatizado nem obtido o (necessário – cf. artigo 7.º n.º 2 da Lei 67/98) consentimento dos titulares dos dados.

Como é óbvio, o que acaba de ser descrito suscita um aspecto novo – que a CNPD ainda não apreciou – e que se prende com a «partilha de informação» relativa a «não dadores de sangue». Os responsáveis dos tratamentos no âmbito dos Serviços de Imuno-Hemoterapia devem notificar a CNPD em relação a estes procedimentos e sobre a forma de partilha de dados na medida em que é claramente questionável que esta informação possa ser partilhada da forma como se sugere.

Pode concluir-se, por isso, que o direito de informação não é assegurado nos moldes em que é exigido pelo artigo 10.º da Lei 67/98, de 26 de Outubro. Muito embora tenha sido referido em alguns hospitais que o simples facto de os utentes constatarem que existem computadores e que alguns dados são aí introduzidos poderia indiciar, pelo menos, a existência de um tratamento, esse facto não é suficiente uma vez que a Lei 67/98 não admite uma «forma implícita» de assegurar o direito de informação.

O direito de informação tem de ser expresso, adiantando a lei que os documentos que servem de base à recolha de dados pessoais «devem conter as informações» necessárias, entre outras, a assegurar o direito de acesso (cf. artigo 10.º n.º 2 da Lei 67/98). Isto é, todos os formulários existentes nos hospitais e que se destinem a recolher dados pessoais junto dos utentes devem ser reformulados por forma a assegurar o direito de informação – nos termos consignados no artigo 10.º n.º 1 e 2 da Lei 67/98 – devendo, ao mesmo tempo, ser obtido o consentimento para o tratamento de dados quando esse consentimento se revelar necessário (cf. artigo 7.º n.º 2 da

Lei 67/98) e o titular dos dados estiver em condições de poder prestar esse consentimento (veja-se o disposto no artigo 7.º n.º 3 alínea a) da Lei 67/98).

Em termos de síntese considera a CNPD que não está a ser dado o direito de informação, nos termos em que é legalmente exigível, sendo conveniente salientar que há situações particulares em que é imprescindível assegurar, com particular cuidado, esse direito em relação à finalidade (v.g. serviços de sangue, telemedicina, investigação científica com dados nominativos), aos destinatários dos dados (v.g. investigação científica, telemedicina, fornecimento de dados a entidades externas) e sobre as condições em que pode ser exercido o direito de acesso e rectificação por parte dos titulares.

Esta informação deverá constar, obrigatoriamente, dos formulários de recolha de dados (cf. artigo 10.º n.º 2), poderá ser objecto de informação verbal sempre que os dados sejam recolhidos por inquérito verbal junto dos titulares, sendo desejável que, nos locais onde tais dados são sistematicamente recolhidos, haja avisos afixados que forneçam tais informações. Quando os dados forem utilizados para investigação científica deverão ser adoptados mecanismos de informação e de consentimento informado (ver infra).

2. No que diz respeito ao ***direito de acesso*** por parte dos titulares não foi possível apurar quaisquer elementos numéricos sobre a quantidade ou percentagem de pedidos formulados. Os hospitais não dispõem desses elementos, mas informam que os pedidos são muito raros. Muitas vezes o que se pretende é o fornecimento de meios auxiliares de diagnóstico ou cópia da ficha clínica para fins de continuidade da prestação de cuidados ou obtenção de uma «segunda opinião», sem estar especificamente em causa o exercício do direito de acesso.

Em relação a 73 aplicações em que foi solicitada informação sobre a forma e entidade junto de quem é exercido o direito de acesso foram obtidos, em 69 respostas, os seguintes resultados:

- o Ao Director de Serviço – 47
- o Ao Director Clínico – 19

- Ao Director do Hospital – 1
- Ao médico que prestou os cuidados – 1
- Ao enfermeiro Chefe⁽⁸⁾ – 1

Ou seja, é patente que o exercício do direito de acesso pode ser feito, como é lógico, junto do Director do respectivo serviço ou junto do director clínico.

De acordo com as respostas dadas – pois nem todos sabiam informar – o acesso aos dados de saúde será conferido mediante «intermediação médica» em 59 casos (88,05%), podendo essa intermediação ser feita através do “médico que prestou os cuidados” ou pelo “director clínico” sempre que o titular não apresente médico da sua confiança. O acesso directo ocorre em 8 casos (11,95%).

3. Verificou-se, no entanto, que alguns hospitais dispõem de regras escritas com vista a assegurar ou delimitar procedimentos atinentes quer ao direito de informação quer ao «direito de acesso» aos próprios titulares. Estes procedimentos, que apresentam como regras orientadoras, nem sempre seguem de perto as regras estabelecidas na Lei 67/98, razão pela qual poderão conter algumas imprecisões ou princípios demasiado genéricos. Por essa razão, será desejável que, com as respectivas notificações à CNPD, juntem esses procedimentos para uma ponderação pela Comissão das regras de acesso à informação.

Consigna-se, num hospital, que importa «garantir adequada informação ao doente ou ao seu legítimo representante sobre os episódios de observação e tratamento ocorridos no Hospital». Para o efeito, o médico assistente responsável pelo episódio elabora o respectivo relatório. Quando exista nota de alta a mesma constitui relatório do episódio. Para execução do relatório o médico assistente pode consultar o processo no arquivo e solicitar cópia dos elementos do processo que entenda necessários. Os relatórios são enviados pela Direcção Clínica ao requerente através do Serviço de Doentes no prazo de 15 dias úteis após o pedido. A cedência

⁽⁸⁾ Trata-se de aplicação relativa a gestão de cuidados de enfermagem prestados em Centro Hospitalar.

de cópias dos documentos constantes do Processo clínico ao doente é feita a seu pedido e após autorização do Director Clínico.

Num outro hospital consigna-se que o acesso ao processo clínico por parte do doente «deve ser feito mediante procedimentos que respeitem os seus direitos, garantam a confidencialidade, tenham em conta a sua capacidade de entendimento e o efeito que o conhecimento da sua doença pode desencadear em termos psíquicos e psicológicos. Será prudente que tal acesso seja feito com acompanhamento médico, sempre que possível o médico assistente do doente».

São definidos os seguintes procedimentos:

- 1) Apresentação de requerimento dirigido ao Conselho de Administração pelo próprio ou por quem legalmente o represente (cf. cópia do formulário);
- 2) O Director de Serviço é o responsável pelo acesso ou por qualquer informação sobre o conteúdo do processo clínico, devendo designar um médico do quadro hospitalar que preste tal informação, sempre por escrito, mesmo quando tenha de a explicar verbalmente ao próprio doente, a solicitação deste;
- 3) Preferencialmente deverá ser o médico assistente a prestar a informação ao doente;
- 4) Existe a possibilidade de o doente indicar pessoa ou entidade a quem devem ser comunicados os dados que lhe dizem respeito;
- 5) Apenas deve ser autorizada a comunicação de informação constante do processo clínico, quando não exista prejuízo para terceiros. Não deve ser prestada a informação clínica completa quando houver informação clínica de outras pessoas, mesmo que familiares, e quando haja fundados receios de que a revelação desses dados possa ser prejudicial para a saúde do doente (v.g. diagnóstico de malignidade em doente instável psicologicamente).

Num outro regulamento estabelece-se que o médico do doente ou o Director de Serviço são os únicos profissionais autorizados a prestar esclarecimentos ou informação a cada doente, ou aos seus familiares directos, e neste caso com o conhecimento ou até autorização daquele.

Sendo o acesso ao processo clínico assegurado de forma indirecta, foi ainda constatado num hospital que o acesso pode ser assegurado através da entrega ao utente do «boletim de alta», do qual consta a «terapêutica» e o «diagnóstico de saída». Porém, em situações pontuais – nomeadamente em caso de diagnósticos de malignidade – foi admitida a possibilidade de alteração do «descritivo do diagnóstico» no boletim de alta, muito embora pudesse ser mantido o «código da patologia». A Direcção do Hospital e o Director Clínico já foram alertados no sentido de que este procedimento é violador do princípio da transparência (artigo 2.º da Lei 67/98) e contraria os princípios relativos ao direito de acesso constante do artigo 11.º da Lei 67/98.

Sendo o acesso assegurado de forma indirecta – por intermediação médica (cf. artigo 11.º n.º 5) – o responsável pode omitir a revelação de alguns dados pessoais. Não pode modificar os «diagnósticos de saída» ou “corrigir” a informação clínica, ainda que se entenda que o faz na «protecção» ou «interesse» do doente.

4. O direito de conhecer os dados que sobre si são tratados assume-se como direito fundamental, já que o artigo 35.º n.º 1 da CRP reconhece esse direito, o qual será exercido nos termos da lei.

O artigo 11.º n.º 5 da Lei 67/98, de 26 de Outubro, estabelece que esse direito é «exercido por intermédio de médico escolhido pelo titular dos dados».

O direito de acesso a dados clínicos não é encarado da mesma forma em todos os países⁽⁹⁾.

Na *Alemanha* a lei organiza o acesso directo do paciente aos dados objectivos do seu *dossier* (resultados de exame, radiográficos, troca de correio entre médicos). O acesso a *elementos subjectivos* pode ser-lhe recusado.

⁽⁹⁾ Relatório apresentado à Assembleia Nacional francesa pelos deputados MM. Claude Evin, Bernard Charles e Jean-Jacques Denis relativo ao «projecto de Lei sobre os direitos dos doentes e a qualidade dos sistemas de saúde (n.º 3258).

Na *Dinamarca* o direito de acesso aplica-se à totalidade das informações que figuram no processo clínico (incluindo as notas pessoais ou os comentários em relação aos exames radiográficos). Cada pedido de acesso é objecto de apreciação e a consulta pode ser directa ou ser efectuada com a ajuda de um médico.

Na *Holanda* é consagrado e reconhecido o direito de acesso directo à totalidade do dossier, salvo às informações susceptíveis de atentar contra a vida privada de terceiros.

Em França, a Lei de 4 de Março de 2002 relativa aos direitos dos doentes e à qualidade dos sistemas de saúde estabeleceu o princípio do acesso directo pelo paciente ao conjunto das informações de saúde que lhe dizem respeito e o Decreto de 29 de Abril de 2002 regulamentou a forma de exercício deste direito⁽¹⁰⁾. No entanto, o paciente pode sempre, se o desejar, aceder aos seus dados através da escolha de um médico da sua confiança.

Em Portugal, o artigo 10.º da Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina – Convenção sobre os Direitos do Homem e a da Biomedicina, ratificada por Decreto do Presidente da República n.º 1/2001, de 3 de Janeiro – consagrou dois direitos: o «de saber» e o de «não querer saber». Efectivamente, o n.º 2 do preceito citado refere, de forma expressa, que “qualquer pessoa tem o direito de conhecer toda a informação recolhida sobre a sua saúde. Todavia, a vontade expressa por uma pessoa de não ser informada deve ser respeitada». Admite o n.º 3 do artigo 10.º que, a título excepcional, a lei «pode prever, no interesse do paciente, restrições ao exercício dos direitos mencionados no n.º 2».

Apresentando-se as limitações ao direito de acesso como excepcionais, será de admitir que a regra geral contida no artigo 11.º n.º 5 da Lei 67/98 pode ter de sofrer uma inflecção. Daí que se considere adequado ponderar, em termos legislativos, se deve continuar a manter-se a regra do «acesso por intermediação». Caberá à Assembleia da República ponderar e legislar sobre esta matéria.

⁽¹⁰⁾ In «Guides de la CNIL»: “Professions de Santé” – Fiches thématiques, pág. 10 (in <http://www.cnil.fr>)

Os pedidos de acesso mais frequentes – e que têm originado maiores dúvidas aos responsáveis – relacionam-se com o acesso de terceiros, no âmbito das mais diversas finalidades⁽¹¹⁾.

3. Respeito pelo princípio da finalidade

Em relação às finalidades dos tratamentos verifica-se que, em geral, os dados pessoais recolhidos são utilizados no âmbito das finalidades especificadas no artigo 7.º n.º 4. São ainda utilizados para outras finalidades compatíveis, nomeadamente para fins de investigação científica ou de saúde pública (cf. doenças de declaração obrigatória).

Como se verá, as objecções que existem prendem-se com o insuficiente cumprimento das condições de legitimidade em matéria de utilização de dados para fins de investigação científica. Neste particular – onde se verifica uma utilização com preterição dos pressupostos que têm sido fixados pela CNPD – importa que os hospitais alterem os seus procedimentos ou que, em alternativa, sejam adoptadas providencias legislativas que facilitem a realização de verdadeiros projectos de investigação científica que decorram de imperativos de interesse público.

O acesso a dados por parte de terceiros (v.g. por parte de familiares, seguradoras, tribunais) pode implicar um desvio da finalidade, muito embora possa ser considerado compatível com a finalidade originária (cf. artigo 5.º n.º 1 al. b) da Lei 67/98). Esta problemática será, porém, analisada quando abordada a temática dos arquivos.

Muito embora se tenha detectado em 2 hospitais que os dados dos dadores de sangue eram utilizados para os felicitar na data do seu aniversário ou enviar-lhe as “Boas-Festas” – sem observância dos princípios relativos ao direito de informação e oposição – não foi detectada a utilização de dados clínicos para qualquer finalidade que possa ser qualificada como incompatível com a finalidade originária.

⁽¹¹⁾ Esta temática será analisada, oportunamente, no âmbito do acesso aos dados do arquivo clínico.

4. A utilização de dados de saúde para investigação científica

1. Não foram encontrados em qualquer hospital tratamentos cujos dados fossem originária e exclusivamente recolhidos para fins de investigação científica. Os dados pessoais tratados pelos hospitais são, originariamente, recolhidos com a finalidade de diagnóstico, prestação de cuidados de saúde e gestão de serviços de saúde, finalidade integrada na previsão do artigo 7.º n.º 4 da Lei 67/98, de 26 de Outubro. O que se verificou foi que muitos médicos – interessados no estudos de casos clínicos ou na realização de investigação científica em relação a certas patologias – pretendem seleccionar e aceder aos processos clínicos dos utentes que consideram poder servir de base aos estudos que se propõem realizar. Os processos são, normalmente, requisitados ao arquivo clínico do hospital.

Se bem que apenas 14 hospitais dos 38 hospitais visitados refiram dispôr de procedimentos escritos em matéria de regras para acesso à informação, são poucos aqueles onde se faz referência à necessidade de observar certas regras para utilização dos processos clínicos com finalidades de investigação científica.

Em matéria de estudos científicos, nem todos os hospitais fazem referência, nos procedimentos escritos, à forma de disponibilização dos processos para esta finalidade. No entanto, alguns dos hospitais admitem o acesso ao processo clínico com o objectivo de “sustentar estudos de carácter científico” por parte dos técnicos de saúde do Hospital e outros que o requeiram. Esta consulta e a utilização dos dados respectivos deve ser feita “com respeito pela privacidade dos doentes envolvidos”. Quando haja motivo fundamentado, refere-se, a Direcção Clínica pode autorizar o «levantamento dos processos para fora do Arquivo», fixando, por despacho, o prazo máximo para a devolução dos processos clínicos.

Um dos regulamentos admite a execução de cópias contra pagamento de montante destinado a suportar os respectivos custos. Quando estiverem disponíveis suportes digitalizados admite-se, igualmente, a possibilidade de a Direcção Técnica ceder cópias do processo clínico.

Um dos regulamentos prevê – no caso de o processo não estar arquivado por motivos de estudo – que os Secretários de Unidade do Serviço de Internamento devem diligenciar por fazer chegar o processo ao Arquivo Clínico, a fim de estar presente no dia da consulta.

Para obviar que sejam facultadas grandes quantidades de processos clínicos, alguns hospitais fixam um número máximo de processos a disponibilizar diariamente aos médicos ou profissionais de saúde que fazem investigação⁽¹²⁾.

Para que os processos possam ser requisitados ao arquivo há outros procedimentos não escritos que devem ser observados e que variam de hospital para hospital, nomeadamente:

- a) A investigação científica pode ser restrita a médicos (ou enfermeiros) do próprio hospital;
- b) A investigação científica deverá ser autorizada previamente por uma ou várias das seguintes entidades: Comissão de Ética, Conselho de Administração, Direcção Clínica ou, mesmo, pelo Director de Serviço onde o médico se encontra inserido;
- c) O médico é obrigado a consultar o processo no arquivo ou o processo clínico não pode sair do arquivo por período superior a 48 horas;
- d) O médico está impedido de requisitar, por cada vez, um determinado número máximo de processos clínicos (máximo 20 ou entre 30 e 50);

2. Quando o Hospital, na qualidade de responsável pelo tratamento, pretender facultar os dados dos doentes para a finalidade de investigação científica deve certificar-se de que essa finalidade foi notificada e autorizada pela CNPD⁽¹³⁾. Isso não tem acontecido porque os processos têm vindo a ser facultados sem qualquer controlo da CNPD. ***Neste particular há um generalizado incumprimento da lei.***

⁽¹²⁾ No Hospital de Santa Cruz «cada médico requisitante só pode solicitar até 20 processos clínicos por dia».

⁽¹³⁾ Não estando essa finalidade prevista no n.º 4 do artigo 7.º as «condições de legitimidade terão que resultar da previsão do artigo 7.º n.º 2 da Lei 67/98. Deste modo, o artigo 28.º n.º 1 al. a) impõe o controlo prévio para o tratamento de dados de saúde para a referida finalidade. Trata-se, por outro lado, de um desvio da finalidade que também carece de autorização da CNPD, nos termos dos artigos 23.º al. c) e 28.º n.º 1 al. d) da Lei 67/98.

A menos que a CNPD entenda que tal realização se fundamenta em *«motivo de interesse público importante indispensável ao exercício das atribuições legais ou estatutárias do responsável»* – o que dificilmente se verifica dado o alcance restritivo que tem vindo a ser dado à previsão do artigo 7.º n.º 2 da Lei 67/98 – o acesso aos dados nominativos dos doentes no âmbito desta finalidade só pode ser facultado se for assegurado o *consentimento dos doentes*. Efectivamente, dada a inexistência de disposições legais que regulem o acesso à informação clínica para fins de investigação científica – ***legislação que deveria ser preparada para viabilizar ou facilitar projectos de investigação de relevante interesse científico*** – a utilização nominativa dessa informação só pode ocorrer por via do *consentimento* (cf. o artigo 35.º n.º 3 da Constituição da República e art. 7.º n.º 2 da Lei 67/98)¹⁴.

Caso não tenha sido obtido o consentimento no momento da recolha ou não seja possível a obtenção posterior do consentimento, o acesso aos dados para esta finalidade só poderá ser feita de forma anonimizada. Caso seja imprescindível o contacto com os doentes terá que ser adoptada metodologia que assegure a informação e consentimento dos doentes com vista à utilização dos seus dados pessoais em projecto de investigação. Foi o que já decidiu a CNPD na *autorização n.º 12/2000, de 25 de Janeiro*⁽¹⁵⁾, que agora sumariamos:

- “1. Tendo presente a necessidade de elaborar amostra aleatória cientificamente correcta o responsável pelo tratamento deve facultar à interessada os dados anonimizados, embora ordenados pelo código do processo e pelas iniciais do doente;
2. Por sua vez, compete à requerente seleccionar a amostra, e uma vez esta seleccionada devolve-a ao responsável pelo tratamento.
3. Cabe ao responsável, subsequentemente, proceder ao contacto dos doentes dela constantes, assegurando o direito de informação e prévio consentimento dos titulares dos dados”.

⁽¹⁴⁾ Cf. Deliberação n.º 13/99, de 16 de Março (*in* Relatório de 1999, pág. 83).

⁽¹⁵⁾ Não publicada. Veja-se no mesmo sentido a Deliberação n.º 202/2002, de 17 de Dezembro, *in* Relatório de 2002.

3. A CNPD verificou que a investigação científica é realizada, em geral, com utilização de dados nominativos dos doentes quando deveria ser o contrário. A investigação devia fazer-se, por natureza, através do recurso a informação anonimizada. Pelo facto de o processo clínico não se encontrar suficientemente informatizado – ou por os responsáveis não terem os sistemas informáticos preparados para fornecerem listagens não nominativas – a investigação faz-se, na quase totalidade dos hospitais, mediante o manuseamento do processo clínico⁽¹⁶⁾. Ora, este tipo de procedimento generalizado *não pode manter-se na medida em que viola vários princípios fundamentais de protecção de dados*:

- a) Os dados pessoais dos doentes são utilizados no âmbito de projectos de investigação científica, sem que aqueles tenham sido informados da possibilidade de os seus dados poderem ser utilizados para esta finalidade (cf. artigo 10.º da Lei 67/98).
- b) Ao ser omitido o direito de informação, o responsável viola elementares princípios de transparência em relação aos doentes, impedindo-os de exercerem qualquer direito de autodeterminação em relação à forma como são utilizados os seus dados (cf. artigo 35.º n.º 3 da CRP e art. 2.º da Lei 67/98). A informação, que é facultada para fins de prevenção, diagnóstico ou prestação de cuidados é desviada, em violação de lei, sem o mínimo conhecimento dos doentes⁽¹⁷⁾.
- c) Os responsáveis violam o princípio da finalidade pois utilizam os dados dos doentes sem que tenham notificado essa utilização ou obtido a necessária autorização da CNPD para aquela finalidade (cf. artigo 5.º n.º 1 al. b) e 28.º n.º 1 al. d) da Lei 67/98).
- d) Caso as pessoas envolvidas no projecto de investigação venham a tratar dados nominativos dos doentes – v.g. para fazer contactos subsequentes (entrevistas ou acompanhamento) – também eles estão obrigados a fazer a notificação deste novo tratamento à CNPD, o que raramente tem vindo a acontecer.

⁽¹⁶⁾ Em 2 hospitais verificou-se que era possível a obtenção de cópia do processo clínico

⁽¹⁷⁾ Os hospitais, no momento em que se questiona a quem pertence a informação inserta no processo clínico, agem como se o doente não fosse o titular dos dados e actuam, pelo simples facto de serem responsáveis dos tratamentos, como se pudessem dispor da informação sem o controlo dos doentes.

Em termos de conclusão final reafirma-se que a forma como estão a ser utilizados os dados dos doentes para investigação científica deve ser objecto de uma ampla reflexão por parte das Administrações dos Hospitais, devendo ser alterados os procedimentos actualmente existentes para os conformar com os preceitos legais. Como responsáveis dos tratamentos, os hospitais não podem alhear-se do controlo de utilização de dados e deixar à mercê daqueles que realizam investigação (médicos, enfermeiros, assistentes sociais, geneticistas, psicólogos, estudantes, professores ou outros profissionais) a faculdade de – em violação dos princípios de protecção de dados – acederem, indevidamente, ao processo clínico do doente.

Também o Governo e Assembleia da República devem reflectir sobre esta problemática, a fim de poderem tomar as medidas legislativas adequadas. A CNPD não ignora que o facto de os projectos de investigação ficarem exclusivamente dependentes do consentimento dos doentes pode inviabilizar ou dificultar a realização e desenvolvimento de projectos de investigação científica relevantes. No entanto, e enquanto não estiverem legalmente previstas outras «condições de legitimidade» a CNPD – *que está vinculada à observância do princípio da legalidade* – deve ater-se, nas suas apreciações, à previsão do artigo 7.º n.º 2 da Lei 67/98.

5. Confidencialidade e regras de segurança

1. Na Deliberação n.º 51/2001, de 3 de Julho⁽¹⁸⁾ a CNPD delimitou o âmbito e alcance do sigilo médico e do dever de confidencialidade. Como aí se referiu, a protecção do segredo médico assenta em motivos de interesse particular (protecção da privacidade do doente), bem como em fundamentos de interesse geral e público (preservação de confiança necessária nas relações médico-doente). O *segredo profissional é a proibição de revelar factos ou*

⁽¹⁸⁾ Disponível in <http://www.cnpd.pt>

acontecimentos de que se teve conhecimento ou que foram confiados em razão e no exercício de uma actividade profissional”⁽¹⁹⁾.

O dever de sigilo abrange, deste modo, todos os factos que tenham chegado ao conhecimento do médico no exercício da sua actividade, ou por causa dela, quando revelados pelo doente ou por terceiro a seu pedido, quando o médico deles se tenha apercebido ou lhe tenham sido comunicados por outro médico. O segredo é uma “condição necessária da confiança dos doentes: é importante que todo o ser humano necessitado de socorro saiba que pode dirigir-se ao médico sem risco de ser traído”⁽²⁰⁾.

O conceito tradicional de sigilo médico - que estabelecia uma relação de confiança na relação directa entre a figura do “médico assistente” e o doente - *relativizou-se* e o sigilo médico assume-se, actualmente, como um «segredo partilhado»⁽²¹⁾ na medida em que o diagnóstico e a prestação de cuidados de saúde é feita em equipa (grupo de médicos no mesmo serviço) ou através da troca de informações entre profissionais de equipas diferentes. Porém, esta partilha institucionalizada de informação deve ser do conhecimento do doente, que poderá manifestar a sua vontade de não querer que determinados dados pessoais, não relevantes para eficácia do trabalho de equipa, sejam revelados.

2. A Lei de Bases da Saúde (Lei 48/90 de 24 de Agosto) considera que «deve ser promovida uma intensa articulação entre os vários níveis de cuidados de saúde, sendo de garantir a circulação recíproca e *confidencial* da informação clínica relevante sobre os utentes» (Base XIII, nº 2). Por isso, de entre os **direitos dos utentes**, assume particular relevância a obrigação de «*respeito pela confidencialidade* sobre os dados pessoais revelados» (Base XIV, al. d). Por força do artigo 6.º n.º 1 al. a) do DL n.º 19/88, de 21 de Janeiro – que aprovou a lei de gestão

⁽¹⁹⁾ Cf. Pareceres da PGR nº 270/78 (in BMJ nº 290, pág. 167) e nº 49/91 de 12/3/92 (in DR IIª S. de 16/3/95, pág. 2938).

⁽²⁰⁾ Cf. neste sentido o parecer da PGR de 12 de Março de 1992, in DR IIª S. de 16/3/95, pág. 2937.

⁽²¹⁾ Cf., para maiores desenvolvimentos, o parecer da PGR de 12/3/92 cit. pág. 2938 e Liliane Dussere, Henry Ducrot e François-André Allaert - "L'Information Médicale: L'ordinateur et la loi", 1996, pág. 23.

hospitalar – um dos princípios que deve nortear a actuação dos órgãos da administração e de direcção técnica dos hospitais do SNS é o do “*respeito pelos direitos dos doentes*”.

O segredo profissional assume particular relevância, igualmente, como obrigação deontológica. O Estatuto da Ordem dos Médicos (aprovado pelo DL 282/77, de 5 de Julho) enuncia como dever dos médicos a obrigação de «guardar segredo profissional (art. 13.º al. c). O Código Deontológico da Ordem dos Médicos⁽²²⁾ tem várias disposições - artigos 67.º a 80.º - sobre segredo profissional e arquivos clínicos. Merecem particular realce as seguintes disposições:

- a) *Artigo 68.º* - O segredo profissional abrange todos os factos que tenham chegado ao conhecimento do médico no exercício do seu mister ou por causa dele;
 - b) *Artigo 69.º* - Os directores, chefes de serviço e médicos assistentes dos doentes estão obrigados, singular e colectivamente, a guardar segredo profissional quanto às informações clínicas que, constituindo objecto do segredo profissional, constem do processo individual do doente organizado por quaisquer entidades colectivas de saúde, públicas ou privadas.
 - c) *Artigo 78.º* - 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.
 - d) *Artigo 122.º* - 1. O médico assistente que envie doente a hospital deve transmitir aos respectivos serviços médicos os elementos necessários à continuidade dos cuidados clínicos.
2. Os médicos responsáveis pelo doente no decurso do seu internamento hospitalar, devem prestar ao médico assistente todas as informações úteis acerca do respectivo caso clínico.

Com base nos preceitos acima citados a CNPD tem entendido que a «partilha da informação clínica» deve ser feita na estrita medida do necessário à prestação de cuidados de saúde, ou

⁽²²⁾ Aceite como integrando princípios regulamentares, mas sem existência jurídica efectiva porque não publicado como diploma do Governo (cf. Parecer da PGR 99/82, in DR II.ª S. de 24/6/82, pág. 4976(1) - 4976(3).

seja, a informação de saúde (vg. o diagnóstico) só deverá ser transmitida quando se revele necessária à prestação de cuidados de saúde ao utente. Daí que se entenda que o facto de todos os profissionais que exercem funções no Hospital (v.g. funcionários administrativos, secretárias de unidade ou do arquivo) se encontrarem vinculados ao segredo profissional não determina que, só por esse facto, tenham livre acesso à informação de saúde dos doentes. O princípio da «confidência necessária» impõe que sejam tomadas medidas técnicas e procedimentais adequadas para evitar que a informação de saúde dos doentes seja restrita àqueles que dela precisam para o exercício das suas funções.

Para ilustrar esta ideia basta referir que em 35,5% das aplicações (não engloba as aplicações do Arquivo e patologia clínica) verificadas não existe «separação lógica» entre dados administrativos e de saúde. Também, no âmbito das aplicações em utilização nos serviços de patologia clínica e Imunohemoterapia, se verificou que, em 70% dos casos, os funcionários administrativos têm acesso ao «diagnóstico possível», seja através dos suportes de papel, seja através das respectivas aplicações instaladas.

3. Todos os profissionais com que contactámos, desde profissionais de saúde a funcionários administrativos, estão conscientes de que manuseiam informação extremamente sensível e protegida pelo segredo profissional.

As regras e procedimentos escritos vigentes em alguns hospitais não deixam de evidenciar os princípios relativos à confidencialidade.

Referem, nomeadamente, que o pessoal “está obrigado a respeitar a confidencialidade dos registos clínicos utilizando o seu conteúdo apenas com o objectivo de tratar ou auxiliar o doente. A informação sobre o doente a facultar a terceiros deve observar o respeito pela confidencialidade dos doentes e deve ser limitada pela “necessidade de saber” desses terceiros para poderem colaborar no tratamento/auxílio ao doente”⁽²³⁾.

⁽²³⁾ Hospital do Barlavento Algarvio e Centro Hospitalar do Funchal.

Não deixam de salientar que se houver condições práticas para tal «deve ser obtido o consentimento prévio do doente ou seu representante para a divulgação de informação sobre o seu estado clínico usando o formulário hospitalar em vigor».

Reafirmando o carácter «absolutamente confidencial» do processo clínico, refere-se que tal obrigação impende sobre «todos os funcionários do hospital independentemente da sua categoria profissional»⁽²⁴⁾, adiantando algumas normas de procedimentos que a violação das regras da confidencialidade é susceptível de «procedimento disciplinar»⁽²⁵⁾.

4. Conforme resulta da Lei 67/98, os responsáveis pelos tratamentos devem pôr em prática medidas técnicas e organizativas adequadas para proteger os dados contra destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, mediante a escolha de níveis de segurança adequados em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger (artigo 14.º n.º 1 e 15.º).

Conforme resulta do Considerando 46 da Directiva 95/46/CE, a protecção dos direitos e liberdades das pessoas passa pelo tipo de “medidas técnicas e organizacionais” tomadas, tanto aquando da concepção do sistema de tratamento como da realização do próprio tratamento. Estas medidas “devem assegurar um nível de segurança adequado, atendendo aos conhecimentos técnicos disponíveis e aos custos da sua aplicação em função dos riscos que o tratamento implica e da natureza dos dados a proteger”.

A necessidade de adopção de medidas de segurança nos sistemas informáticos⁽²⁶⁾ resultou de duas exigências fundamentais: do interesse de os próprios responsáveis hospitalares que não querem ver os seus sistemas devassados por terceiros – podendo colocar em risco o segredo médico e perder a confiança dos doentes – ou de uma imposição legal que assumiu especial relevância a partir do momento em que se enveredou pela regulamentação do tratamento de

⁽²⁴⁾ Hospital de Santarém.

⁽²⁵⁾ Hospital de Santo António do Porto.

⁽²⁶⁾ A lei da criminalidade informática – Lei 109/91, de 17 de Agosto – define «sistema informático» como o “conjunto constituído por um ou mais computadores, equipamentos periféricos e suporte lógico que assegura o processamento de dados».

dados pessoais. As preocupações do legislador centram-se na ideia de que só faz sentido autorizar o tratamento de dados se os responsáveis garantirem que os mesmos estão convenientemente protegidos contra perdas, devassas ou acessos indevidos de terceiros, podendo completar a segurança com sistemas de alarme ou de registos que permitam alertar para tentativas de intrusão (veja-se a parte final do artigo 7.º n.º 4).

5. Alguns hospitais (14) referem ter procedimentos escritos que visam a adopção de regras de acesso e mecanismos que garantam a segurança da informação inserta nos processos clínicos. Nem todos chegaram a enviar aqueles procedimentos escritos.

Nalguns desses procedimentos alertam-se os utilizadores para a necessidade de usar os recursos do hospital de acordo com essas regras e lembra-se que as *passwords* asseguram o acesso à rede e respectivas aplicações informáticas, definindo o «nível de acesso de cada utilizador»⁽²⁷⁾.

Neste contexto, o uso adequado dos recursos informáticos do Hospital proíbe os utilizadores de:

- ❑ Violar as áreas de acesso de outros utilizadores;
- ❑ Tentar a descodificação (*cracking*) de *passwords*;
- ❑ Ler ou modificar a informação de outros utilizadores a que se tenha ocasionalmente acesso;
- ❑ Criar bases de dados próprias sem autorização e sem ligação ao Serviço de Informática;
- ❑ Instalar programas “piratas” nos computadores da instituição;
- ❑ Substituir qualquer computador da instituição por um computador pessoal (particular), ligando-o à rede.

Deste modo, existem responsabilidades específicas para os utilizadores:

- ❑ Não devem revelar *passwords* e estão obrigados a alterá-las periodicamente;

⁽²⁷⁾ Veja-se o documento do Hospital do Barlavento Algarvio que define a «Política de Gestão da Rede Informática do Hospital» e respectivas «normas de procedimentos» de 9/8/2002.

- ❑ Não devem deixar os terminais ou computadores ligados sem utilização (durante mais de 30 minutos), sob pena de serem desconectados da rede. Sempre que o utilizador se ausentar do seu local de acesso ao sistema, deve sair da aplicação onde a sua palavra de passe está registada, por forma a cumprir as regras do sigilo profissional.
- ❑ Não devem deixar o *login* ligado quando saem do posto de trabalho e devem verificar sempre se é o seu *login* que está inserido no computador, antes de começarem a trabalhar;
- ❑ Quando notem um acesso anterior que lhes pareça estranho ou que não tenha sido a própria pessoa a aceder, deverão comunicar imediatamente tal facto aos administradores da rede.

Outros hospitais instituíram procedimentos que visam garantir a segurança através de vários mecanismos específicos ou definição de uma «Política de segurança dos dados»⁽²⁸⁾. De entre esses procedimentos foram enunciados os seguintes

1. Existência de utilizadores com diferentes níveis de acesso;
2. Atribuição de palavras chave;
3. Servidores com acesso físico e lógico restrito;
4. Rede informática estruturada;
5. Implementação de redes virtuais – VLAN'S;
6. Existência de *Fire Wall*;
7. Disponibilização restrita de serviços que diminuem a segurança de dados (ex. internet, e-mail...);
8. O conhecimento da palavra-chave de administradores de servidores é só do conhecimento do responsável pela manutenção dos mesmos;
9. Alteração periódica das palavras-chave;
10. Uso de palavras-chave de *hardware* e *software*;

⁽²⁸⁾ Veja-se o documento «Política de Segurança de Dados», produzido em 26 de Maio de 2003, pelo Hospital de São Marcos – Braga.

11. Realização obrigatória de cópias de segurança dos dados informatizados;
12. Acesso aos sistemas de informação só com autorização prévia;
13. Partilha de dados só mediante autorização;
14. Instalação autorizada de *software*.

Para obter o acesso às aplicações é necessário, em geral, fazer um pedido formal (por impresso) de atribuição de *password*. A atribuição da *password* terá em conta a categoria profissional e as funções desempenhadas, podendo o responsável do serviço a que pertence o utilizador ser ouvido em relação à definição do perfil.

Para uma melhor sistematização dos níveis de acesso há quem estabeleça uma tabela que define o «Grupo de Utilizadores»⁽²⁹⁾.

Em geral, cada posto de trabalho está preparado para aceder única e exclusivamente à aplicação que serve o respectivo serviço onde o utilizador está integrado, através de *login* e *password*.

Alguns procedimentos escritos enunciam, com simplicidade, as 3 fases por que passam os acessos à rede⁽³⁰⁾:

- a) De identificação: quem és?
- b) **De autenticação:** *prova-o* (através de palavra de passe) e diz «*o que és*» (médico, enfermeiro, administrativo);
- c) **De autorização:** *ao que vens* (criar, ler, eliminar ou modificar).

Estes procedimentos escritos são expressos, por regra, em relação à natureza das *passwords*: são pessoais e intransmissíveis⁽³¹⁾. Em consequência, sempre que o funcionário deixe de prestar funções no hospital o chefe ou responsável do serviço deve informar esse facto ao departamento de informática para desactivação da respectiva palavra de passe.

⁽²⁹⁾ Hospital de Santa Luzia (Elvas).

⁽³⁰⁾ Centro Hospitalar do Funchal.

⁽³¹⁾ Hospital do Barlavento Algarvio e Amato Lusitano.

São estabelecidos, igualmente, procedimentos específicos em relação à realização de *backup's*⁽³²⁾.

Para conferir maior segurança, há quem faça auditorias aos sistemas de informação: diariamente «são analisados os históricos dos sistemas, pelo administrador ou operadores de sistema, por forma a efectuar rastreio e detecção de intrusões»⁽³³⁾.

Para assegurar uma maior vinculação do trabalhador à observância dos procedimentos de segurança há quem tenha optado por obrigar o utilizador a assinar um «*acordo de utilização do sistema informático*»⁽³⁴⁾. Dele consta nomeadamente, a impossibilidade de «instalar *software* nos computadores do Hospital» e sujeição dos procedimentos dos utilizadores ao controlo dos serviços de informática.

Verificou-se, porém, que nem todas as aplicações analisadas garantem os adequados procedimentos e regras de segurança. Em relação às *passwords* podemos adiantar que, em relação a um total de 172 aplicações, 158 tinham *password* e 14 não tinham. Em relação à existência de *backups* os números são muito similares.

Em 2 hospitais foram encontradas *passwords* visíveis insertas em auto-colantes junto aos postos de trabalho. Em algumas situações foi afirmado por certos utilizadores que «normalmente a *password* é o meu nome».

Entende a CNPD que os hospitais devem investir mais na formação e sensibilização dos utilizadores por forma a evitar que ocorram «falhas» ao nível da segurança dos sistemas. Por outro lado, é desejável que sejam adoptados procedimentos escritos claros que definam regras de acesso à informação, critérios que definam a atribuição de *passwords*, obrigatoriedade de alteração de *passwords* com determinada periodicidade, bem como a adopção de procedimentos técnicos que obriguem os utilizadores a digitar de novo o seu *login* e *password*

⁽³²⁾ Hospitais do Barlavento Algarvio, de Santa Cruz e de Santa Luzia (Elvas).

⁽³³⁾ Centro Hospitalar do Funchal.

⁽³⁴⁾ Hospital Amato Lusitano

sempre que a aplicação, uma vez «aberta», não tenha sido utilizada durante um determinado período de tempo (v.g. 15 minutos).

6. Prazo de conservação da informação de saúde

A Lei 67/98, dispõe que devem ser tomadas medidas adequadas para assegurar que sejam apagados ou rectificados os dados inexactos ou incompletos, tendo em conta a finalidade para que foram recolhidos ou para que são tratado posteriormente (cf. artigo 5.º n.º 1 al. d). No mesmo contexto, a alínea e) do mesmo preceito dispõe que os dados devem ser «conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior».

No que diz respeito aos *prazos de conservação* dos dados verificou-se que os hospitais não fixaram prazos de conservação da informação, nem têm preocupações particulares nesse domínio. Em geral, verificou-se que os dados são guardados por tempo indeterminado e, em alguns casos são colocados em ficheiro histórico por falta de capacidade dos discos para manterem toda a informação *on line*.

Em 136 aplicações onde tal aspecto foi questionado, verifica-se que apenas duas têm prazos de conservação fixados nos termos da lei, sendo os restantes dados guardados por tempo indeterminado.

Importa sublinhar que, a menos que haja disposição específica sobre prazos de conservação de dados⁽³⁵⁾, deverão os hospitais observar as disposições e prazos de conservação estabelecidos na Portaria n.º 247/2000, de 8 de Maio.

⁽³⁵⁾ O Decreto Regulamentar n.º 16/95, de 29 de Maio estabelece um prazo mínimo de conservação de 50 anos em relação à conservação de dados e documentos relativos a transfusões de sangue. Em relação à actividade dos laboratórios que prossigam actividades de diagnóstico, de monitorização terapêutica e de prevenção no domínio da patologia humana, o Decreto-Lei n.º 217/99, de 15 de Julho estabelece um prazo mínimo de 5 anos para conservação dos resultados nominativos dos exames analíticos.

III. CONSIDERAÇÕES GERAIS SOBRE O TRATAMENTO DE INFORMAÇÃO DE SAÚDE NOS HOSPITAIS

1. Rede hospitalar e gestão da informação de saúde

1. Os hospitais estão hoje dotados, na generalidade dos casos, de uma rede que cobre todo o Hospital. Dos 38 hospitais visitados verifica-se que 34 informam que a rede cobre todo o hospital e apenas 4 referem que a rede não cobre todos os serviços. Há situações muito pontuais em que é anotada a necessidade de melhorar a rede eléctrica, a velocidade ou largura de banda da rede informática para poder ser dada uma resposta eficaz às exigências do serviço, nomeadamente em termos de eficácia da sua Intranet.

Perante esta constatação entende-se que, em geral, os Hospitais estão tecnicamente preparados para poderem evoluir para a adopção de um *dossier clínico informatizado* e para a criação de mecanismos de circulação da informação em rede que, como adiante se verá, podem garantir de forma mais eficaz a confidencialidade da informação tratada em relação aos doentes.

2. Em relação às aplicações utilizadas verifica-se que, à excepção dos Hospitais dos SAMS, do Hospital das Descobertas e dos estabelecimentos da saúde das Regiões Autónomas, o sistema de informação assenta, em geral, na aplicação informática concebida pelo IGIF – aplicação “SONHO”. Trata-se de uma aplicação especialmente vocacionada para o registo de dados administrativos (identificação, gestão de doentes e de consultas), a qual tem particular utilização – pela inexistência de outras aplicações – em hospitais de pequena dimensão. Esta aplicação “SONHO” é também utilizada em 80% dos hospitais para a gestão da actividade do arquivo clínico: escolha de processos clínicos destinados à consulta, gestão do arquivo e gestão de requisição de processos (entradas e saídas no arquivo).

Não se notou um grande entusiasmo por parte dos utilizadores em relação ao manuseamento da aplicação, apontando-lhe como ponto fraco o seu carácter pouco amigável e a pouca utilidade já que não faz a gestão da informação clínica.

Já se encontra instalada em alguns hospitais (em fase de exploração ou em fase experimental) a nova aplicação do IGIF denominada “SAM” (*Sistema de Apoio ao Médico*), a qual está vocacionada para a gestão da informação clínica e acompanhamento dos actos médicos. Segundo nos foi informado dispõe esta aplicação, ainda, de ferramenta que permite fazer – em tempo real – os pedidos de análises clínicas e a consulta dos respectivos resultados. Os profissionais que se pronunciaram sobre esta aplicação manifestaram o seu agrado em relação ao seu manuseamento e generalização pelos hospitais, qualificando-a como um instrumento muito útil e necessário à gestão da informação clínica. Foi possível constatar, em alguns hospitais (v.g. urgência), que os médicos manuseiam com especial agrado esta aplicação e salientam, em termos de eficácia e convivialidade, as melhorias que ela representa em relação ao «SONHO». Para além da inserção dos dados de saúde foi referenciada a vantagem de permitir a gestão da prescrição e a emissão da receita.

Existe uma política muito diversificada em relação à organização do sistema de informação hospitalar. Como se referiu, os hospitais de pequena dimensão servem-se das aplicações concebidas pelo IGIF (“SONHO”, “ASIS” e GDH’s), só recorrendo à aquisição de aplicações a empresas privadas em situações de manifesta necessidade (v.g. no âmbito da gestão de análises clínicas).

Os hospitais de maior dimensão procuram aproveitar as aplicações do IGIF e tentam, gradualmente, fazer a informatização dos diversos serviços na medida em que as disponibilidades financeiras o permitem.

Nos hospitais mais recentes, porque criada uma rede estruturada para atingir objectivos que apontam para uma informatização integrada, nota-se um esforço para assegurar a informatização integral do processo clínico. Para o efeito, as aplicações são concebidas de raiz (e à medida) para atingir esse objectivo e alargadas, gradualmente, aos vários serviços à

medida que são concebidos os respectivos «módulos» que contemplam as necessidades de gestão da informação clínica de cada serviço (v.g. Hospital das Descobertas, de S. Maria da Feira e Amadora/Sintra).

Anota-se que, ao nível das Regiões Autónomas, existem especialidades em relação ao continente. No Centro Hospitalar do Funchal existem aplicações autónomas de gestão da «ficha clínica» para anotar os cuidados a cargo dos médicos ou dos enfermeiros. Acresce, por outro lado, que alguma informação automatizada constante da ficha médica ou de enfermagem pode ser partilhada com os Centros de Saúde (v.g. vacinas, análise, notas de alta). Existe, assim, um suporte único para cada doente que pode ser partilhado.

Também ao nível da Região Autónoma dos Açores se constata que os Centros de Saúde (Vila Franca do Campo e Ribeira Grande) prestam cuidados de saúde no âmbito da urgência e internamento, razão pela qual foram objecto da visita da CNPD e de análise neste documento. Nos hospitais cujo «registo base» assenta na aplicação “SONHO” vão sendo concebidas (através dos seus recursos ou com recurso a meios externos) ou adquiridas a empresas privadas aplicações que – obtendo os dados administrativos da aplicação “SONHO” – estão vocacionadas para fazer a gestão da informação clínica de cada serviço.

Porém, no domínio da informatização dos vários serviços assiste-se a uma evolução muito diversificada de hospital para hospital, muitas vezes influenciada por vários factores: pela especial sensibilidade e iniciativa dos médicos que pertencem ao serviço e que apostam na utilização dos suportes informáticos, em função dos meios técnicos disponíveis, em função da importância e relevância que o serviço representa no contexto do hospital ou pela necessidade de tratar, de forma estruturada, determinado tipo de informação.

Verifica-se, muitas vezes, que serviços contíguos estão muito longe um do outro em matéria de utilização das novas tecnologias. Ao lado de um serviço que se encontra totalmente informatizado pode funcionar um outro que gere o *dossier* clínico, em exclusivo, através do recurso a suportes de papel.

3. A sensibilização dos profissionais de saúde para a utilização das novas tecnologias é um factor determinante e decisivo para a utilização de aplicações informáticas.

Se bem que haja hospitais que atribuíram *password* a todos os médicos, foi possível constatar que em alguns hospitais de grande dimensão, que havia um reduzido número de médicos (menos de 5%) que tinham *password*. Também há hospitais (2) que informaram que todos os médicos têm *password*. Porém, o facto de os médicos terem *password* não significa que utilizem as aplicações no respectivo serviço.

Por exemplo, foram disponibilizados dados de 2 hospitais sobre o grau de acesso de médicos à rede e que são ilustrativas do grau de utilização das aplicações:

1.º exemplo:

Médicos com acesso à rede – **189** (59%);

Médicos que não acedam à rede – **130** (41%);

Enfermeiros que acedem à rede – **619** (72%);

Enfermeiros que não acedem à rede – **235** (28%).

2.º exemplo:

Médicos activos (com palavra-chave) – **916**;

Médicos que fizeram, pelo menos, **1 registo** – **70** (7,64%).

Parece-nos que o entusiasmo dos profissionais em relação à utilização das aplicações também depende, em grande medida, da utilidade que estas apresentam para o exercício da sua actividade profissional.

Por isso, naqueles hospitais onde tem vindo a ser introduzida a aplicação “SAM” nota-se um maior interesse e entusiasmo dos profissionais de saúde na obtenção de *passwords*, verificando-se, em consequência, um aumento da utilização do sistema. Este facto demonstra que as aplicações informáticas cativam os utilizadores sempre que estes vêem nelas um instrumento que lhes permite obter ganhos em termos de eficácia, de produtividade, melhor

sistematização ou acesso à informação. No mesmo contexto, também se assiste, da parte da direcção de alguns hospitais, a um esforço no sentido de instalar aplicações de gestão de doentes como forma de «incentivar» ou, até, «obrigar» os profissionais de saúde a utilizar aqueles meios por serem mais eficazes em termos de sistematização da informação, de eficácia no funcionamento do serviço ou, ainda, por conferirem um melhor e mais rápido apoio ao médico em termos de celeridade na consulta ou de disponibilidade da informação clínica.

Muito embora se diga e se reconheça que nem todos os profissionais de saúde estão sensibilizados para a utilização da informática – tal como acontece no âmbito de outras actividades profissionais – a verdade é que nos hospitais e serviços onde os suportes automatizados dominam sentimos que os profissionais de saúde têm aderido gradualmente à utilização das novas tecnologias⁽³⁶⁾. Talvez se possa concluir que a informatização dos serviços se apresenta como um desafio à mudança, a qual contribui, de forma decisiva, para – em matéria de protecção de dados – conferir especial protecção à confidencialidade da informação clínica.

Mercê de uma certa iniciativa de alguns profissionais de saúde ou da vontade de melhorar a capacidade de resposta⁽³⁷⁾, constatou-se em alguns hospitais que determinados serviços se encontram totalmente informatizados, com aplicações em computadores isolados ou em rede, e que a gestão da informação do serviço é exclusivamente processada nesses equipamentos. De hospital para hospital foi possível apercebermo-nos que, conforme os serviços, esta forma de

⁽³⁶⁾ Para suprir algumas dificuldades práticas a CNPD tem entendido que embora o acesso à informação de saúde deve ser de acesso restrito aos médicos (cfr. Base n.º XIV n.º 1 al. c) e d) da Lei de Bases da Saúde - Lei n.º 48/90, de 24 de Agosto, e artigo artigos 67.º e 68.º do Código Deontológico da Ordem dos Médicos) ou a outros profissionais de saúde, obrigados a sigilo profissional - nomeadamente os enfermeiros – admite-se que outros profissionais (v.g. administrativos) possam, sob o seu controlo, instruções e orientação, ser mandatados para - em seu nome - aceder aos dados de saúde (cf. neste sentido a Deliberação n.º 36/2000, de 14 de Julho, *in* Relatório de 2000, pág. 100).

⁽³⁷⁾ Esta constatação – reportada a vários hospitais – não deixou de ser referida em relação a um Hospital por parte de uma empresa especializada – a World Software Services – que fez a avaliação do seu sistema de informação, em documento que nos foi facultado. Aí se refere, a este propósito, que «os serviços de gestão dos SI não conseguem prestar o suporte adequado aos utilizadores, criando situações de baixo nível de satisfação e deixando campo livre para o surgimento de iniciativas particulares nesta área».

gestão da informação se pode apresentar como «autónoma» em relação aos restantes serviços do hospital.

Se é verdade que, em geral, estas iniciativas estão integradas num esforço da Direcção que visa assegurar uma melhor estruturação da informação, também foi possível constatar que em algumas situações a Direcção do Hospital ou os responsáveis da informática suspeitam (ou sabem) da existência de certas aplicação a serem utilizadas por médicos, mas não tomam medidas «clarificadoras», apesar de haver instruções genéricas que não permitem a instalação de *software* não licenciado⁽³⁸⁾.

Pelo elevado grau de detalhe das aplicações, toda a informação clínica é pormenorizada (vg. serviços de cardiologia e obstetrícia), sendo de supor que raramente consta da ficha clínica em papel, nomeadamente nos casos em que aqueles serviços se assumem como «responsáveis» do tratamento⁽³⁹⁾. Quando existe um elevado «grau de autonomia» ou «independência» do serviço que utiliza, em exclusivo, determinadas aplicações há uma certa dúvida quanto à «titularidade» e «responsabilidade» da aplicação, facto que contribuiu para a omissão de notificação da mesma à CNPD.

Muitas vezes é a própria direcção do hospital que questiona a «titularidade» ou «propriedade» da aplicação como questão prévia em relação à omissão da obrigação de notificação. Admitem a existência de aplicações a serem utilizadas pelos médicos, mas não se querem «intrometer» ou «entrar em confronto» com aqueles profissionais. Porém, não se dão conta de que pode estar a ser tratada informação excessiva ou sem as necessárias regras de segurança. Para ilustrar esta ideia basta referir que foram encontradas algumas destas aplicações a funcionar nestas circunstâncias: não tinham *password* (ou a *password* única era partilhada por todos os profissionais do serviço⁴⁰), não faziam a separação lógica entre dados administrativos e de saúde, não eram feitas cópias de segurança. Pelo menos num caso em que não eram feitas

⁽³⁸⁾ Alguns directores de informática referiram que fazem visitas de rotina aos postos de trabalho para verificar a instalação de novo *software*.

⁽³⁹⁾ Em alguns casos porque foi por intermédio de profissionais de saúde do serviço que foram concebidas essas aplicações.

⁽⁴⁰⁾ Num caso a *password* estava colada no écran do computador.

cópias de segurança, foi-nos referido que a aplicação fazia a gestão da informação do serviço, sem que houvesse suportes de papel. Há que reflectir sobre situações deste tipo e pensar seriamente nas consequências que podem advir para os doentes se os equipamentos – muitas vezes já antigos – avariarem de forma irreparável.

Mas deve ser reconhecido, por outro lado, que a par daquelas experiências, *que devem ser banidas ou corrigidas*, foram encontradas – em maior número – iniciativas individuais meritorias e de grande qualidade que apostam na informatização integrada do serviço, com cumprimento integral de regras de segurança e com preocupação absoluta de cumprimento das regras de confidencialidade, muitas vezes apresentando-se como modelo a seguir no próprio ou noutros hospitais.

A dúvida que pode ser suscitada é a de saber em que medida essas iniciativas podem ser compatibilizadas com as aplicações existentes e como podem os dados ser integrados no sistema de informação do hospital. Temos sérias dúvidas que estas aplicações – agora qualificadas como meritorias – não venham a causar dificuldades em relação à concepção integrada dos sistemas de informação nos hospitais.

A verdade é que a CNPD não pode deixar de salientar que, perante a dúvida colocada, *não podem continuar a ser instaladas aplicações informáticas de gestão da prestação de cuidados de saúde sem o seu controlo* em estabelecimentos hospitalares que prestam um serviço público – sabendo-se que o utente celebra um contrato com o hospital – pelo simples facto de ser questionada a responsabilidade pela notificação. Muito menos pode ser invocada a «titularidade privada» por parte do médico de qualquer serviço, com a justificação de que se trata de uma aplicação «própria» ou que se destina a «uso pessoal ou doméstico».

4. A questão que antecede não é nova e a CNPD já teve oportunidade de sobre ela se pronunciar em relação à utilização de aplicações em Centros de Saúde⁽⁴¹⁾. Tratava-se de médicos que utilizavam uma aplicação que consideravam «sua» porque destinada à gestão da informação clínica dos «seus» doentes.

⁽⁴¹⁾ Vejam-se as Deliberações n.º 10/2001, de 13 de Março e Deliberação n.º 45/2004, de 9 de Março.

O problema que deve ser equacionado é o de saber quem deve ser o «responsável pelo tratamento» quando os dados de saúde são processados num serviço público ou em empresas (v.g. sociedades anónimas) quando estão em causa dados dos utentes desses estabelecimentos processados com finalidades de medicina preventiva, diagnóstico e prestação de cuidados de saúde.

Conforme entendimento da CNPD⁽⁴²⁾, a expressão «uso pessoal ou doméstico» não pode ser interpretada no sentido de permitir o tratamento de dados pessoais no interior de uma empresa. Este ponto de vista foi também sufragado pelo STA⁽⁴³⁾ ao considerar que a expressão *uso pessoal ou doméstico* «só pode querer referir-se aos ficheiros contendo informações exclusivamente destinadas a uso por pessoa individual ou no âmbito doméstico (no sentido restrito de domicílio familiar)». Por isso, os tratamentos realizados em hospital não podem ser englobados no âmbito do exercício de actividades exclusivamente pessoais ou domésticas, razão pela qual é aplicável ao seu tratamento o regime da Lei 67/98, de 26 de Outubro (cf. artigo 4.º n.º 2), com a consequente obrigação de notificação à CNPD (cf. artigo 27.º).

A Lei 67/98, de 26 de Outubro, estabelece – no artigo 3.º al. d) – o conceito de responsável: será a “pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem determine as finalidades e os meios de tratamento de dados pessoais”.

Em relação aos tratamentos em causa não é legalmente admissível que o responsável por tratamentos de dados seja uma pessoa que não dirige, não representa nem se responsabiliza pela gestão dos serviços. A decisão sobre a forma de tratamento de dados, as estratégias a utilizar, as finalidades, os dados a tratar e o tipo de acesso aos dados têm que ser definidos pela entidade máxima do serviço.

Prevendo a Lei 67/98 que determinado «serviço» pode apresentar-se como «responsável» admite-se que, em função da autonomia e forma de organização de determinado serviço no contexto da forma como está estruturada a organização, esse serviço possa vir a notificar o

⁽⁴²⁾ Deliberação n.º 32/96, de 4 de Junho (in 3.º Relatório da CNPD, 1996, pág. 235).

⁽⁴³⁾ Acórdão de 5 de Junho de 1997 – Rec. N.º 41023

tratamento na qualidade de «responsável». Essa é uma questão que terá que ser equacionada, desde logo, no seio da instituição hospitalar⁽⁴⁴⁾. Mas, a responsabilidade pela omissão será sempre imputável ao hospital.

O que não é admissível é que um médico se arrogue como sendo o «responsável» pela aplicação informática, utilizada para gestão da informação de saúde no interior de determinado serviço, e muito menos que se apresente como «dono» da informação registada ou que reclame a «titularidade privada» da aplicação.

O que se trata neste caso é de uma iniciativa individual do médico (ou do conjunto de médicos de um serviço) que – sob sua conta e risco – resolveu fazer um tratamento de dados em relação aos doentes que se dirigem ao serviço onde presta serviço. Para além de, como se viu, tal entendimento não ter apoio na previsão da Lei 67/98, este tipo de procedimento tem consequências práticas que não são admissíveis. Várias questões se podem colocar: no caso de o médico que se intitula de «responsável» abandonar o «serviço» qual o destino que vão ter os dados pessoais? O médico pode “levar” estes dados? Com que legitimidade? Pode tratar os dados para outras finalidades (v.g. investigação científica)? Qual o papel do doente em todo este processo?

Como referimos, os doentes forneceram os dados ao Hospital – com quem celebraram um contrato de prestação de serviços de saúde – e estão confiantes que o Hospital preservará os seus dados por forma a que apenas possam ser utilizados na continuidade de prestação de outros cuidados de saúde na mesma instituição.

Por isso, entende a CNPD que, à luz da Lei 67/98, de 26 de Outubro, não é legalmente admissível que um médico do Hospital (ou o conjunto de médicos de um serviço) possa fazer tratamento de dados administrativos e de saúde de utentes daquele estabelecimento, em aplicação que considera «sua» (furtando-se ao controlo do Hospital ou do Serviço em que está

⁽⁴⁴⁾ Importa sublinhar, para além de tudo, que, em sede de «direito de informação», a entidade que trata os dados está obrigada a assegurar o necessário esclarecimento sobre a identidade do responsável pelo tratamento (cf. artigo 10.º da Lei 67/98).

integrado) invocando o facto de ter sido por si concebida ou, a seu pedido, por pessoa ou entidade externa ao Hospital.

Em situações deste tipo só uma solução alternativa se admite:

- a) Haver um acordo entre o médico e o Hospital que garanta que a informação processada apenas pode ser tratada no interior do Serviço (ainda que possa ser partilhada por outros Serviços do Hospital no contexto da necessidade de assegurar a continuidade de prestação de cuidados). Deve ser garantido que, em caso algum, nenhum médico do serviço pode «apropriar-se» da informação, para fins estritamente privados. A aplicação deve ser notificada à CNPD, sendo responsável o Hospital ou o Serviço onde se encontra instalada a aplicação.
- b) Se não houver acordo e o médico continuar a reclamar a «titularidade privada» da aplicação entende-se que o tratamento em causa deve cessar, ainda que devam ser adoptadas metodologias de recuperação da informação para assegurar a continuidade de prestação de cuidados de saúde aos utentes do serviço.

Por isso, *a CNPD alerta os hospitais para a necessidade de fazerem um levantamento exaustivo de todas as aplicações de gestão de informação de saúde, optando por uma das soluções acima preconizadas*. A CNPD lembra, mais uma vez, que o tratamento de dados com omissão de notificação é passível de sanções pecuniárias (coimas) ou susceptível de constituir infracção criminal.

2. A utilização de sistemas de Videovigilância

Em geral, os sistemas de videovigilância estão instalados nas entradas, corredores, acesso a elevadores e a determinados serviços. Estes sistemas estão especificamente direccionados para a «protecção de pessoas e bens», funcionando muitas vezes como meios complementares da actividade desenvolvida por profissionais pertencentes a empresas de segurança privada.

Nos 38 hospitais visitados, encontravam-se instalados tais sistemas em mais de 50% (em 21 hospitais), sendo de salientar que apenas 4 hospitais notificaram esses tratamentos à CNPD. Ou seja, 17 tratamentos funcionavam sem o necessário *controlo prévio*, tendo-se verificado algumas anomalias na sua utilização.

Efectivamente, em alguns hospitais os sistemas estavam dotados de *cameras* rotativas a 360 graus, o que permitia a captação de imagens em prédios contíguos. Num outro hospital foi constatado que as imagens poderiam ser acessíveis aos funcionários – mediante simples solicitação escrita à Direcção do Hospital – para detectar eventuais danos em veículos estacionados na zona limítrofe do Hospital, que servia de estacionamento.

Importa ter presente que o acesso indiscriminado às imagens, nomeadamente se captarem a entrada de pessoas em determinados serviços, pode consubstanciar um desvio da finalidade (porque passível de documentar informação de saúde das pessoas filmadas) e envolver a violação da sua privacidade ou, mesmo, contribuir para a sua discriminação. Todos estes aspectos não podem deixar de ser considerados pelos hospitais no momento da instalação dos sistemas.

Acresce, por outro lado, que em vários hospitais não é sequer assegurado o direito de informação, legalmente exigido, em relação à recolha de imagens. Como decorre da lei, *o direito de informação deve ser assegurado através da colocação de avisos*, em locais bem visíveis (v.g. entradas do Hospital, corredores, junto aos elevadores), que alertem para a captação/gravação de imagens e respectivas finalidades.

Constatou-se, igualmente, terem sido instalados sistemas de videovigilância no interior de alguns serviços (v.g. obstetrícia/berçários e corredores) com o objectivo de vigiar o movimento de pessoas no seu interior.

A instalação destes sistemas – especialmente vocacionados para detectar a entrada de pessoas estranhas ao serviço – deve sempre preservar a intimidade dos doentes. As imagens gravadas não devem ser visionadas, limitando-se os responsáveis a entregá-las às autoridades policiais sempre que haja suspeita ou participação da prática de crimes.

É fundamental que os Hospitais notifiquem os tratamentos, especificando com rigor quais as finalidades prosseguidas e as condições concretas em que são captadas as imagens para permitir à CNPD – no âmbito das suas competências de *controlo prévio* (cf. artigo 28.º n.º 1 al. a) da Lei 67/98) – fixar algumas das condições necessárias a preservar a confidencialidade dos titulares dos dados.

IV. ASPECTOS PARTICULARES VERIFICADOS

1. As experiências de Telemedicina

1. De entre os 38 hospitais visitados constatou-se que 21 tinham experiências de telemedicina. *Alguns hospitais utilizam a telemedicina em várias especialidades clínicas*, colaborando quer com hospitais quer com clínicas privadas, verificando-se no total, e de acordo com as informações obtidas em cada um dos hospitais, a existência de 54 experiências de telemedicina. Isto é, alguns hospitais utilizam o equipamento no âmbito de várias especialidades clínicas.

Nenhuma destas experiências de telemedicina se encontra notificada à CNPD, facto que explica um desconhecimento generalizado sobre as regras de segurança adoptadas, a inexistência de quaisquer regras escritas ou cláusulas de responsabilidade decorrentes de um eventual erro de diagnóstico, bem como a adopção de procedimentos para assegurar o direito de informação dos doentes.

As experiências de telemedicina envolvem, em concreto, várias especialidades clínicas: fisiatria, neurologia e neuroradiologia, ortopedia, dermatologia, cirurgia, cardiologia e cardiologia pediátrica, anatomia patológica, gastroenterologia, genética, imagiologia, radiologia, obstetrícia, pneumologia, psiquiatria.

2. Foram facultados 2 relatórios relativos a 2 hospitais que abordam a experiência em telemedicina.

No *Hospital de Santa Luzia de Elvas* verifica-se que, no ano de 2003, foram atendidos um total de 533 utentes, distribuídos pelas seguintes idades: até aos 20 anos (57); dos 20 aos 40 (125); dos 40 aos 60 (145), mais de 60 (205).

Em termos de especialidades a distribuição foi a seguinte: cirurgia (221), dermatologia (161), neurologia (7), fisioterapia (32), oncologia (12), ortopedia (100).

Em relação ao *Hospital de Serpa* – que faz consulta nas especialidades de fisioterapia, neurologia, ortopedia e dermatologia – foram atendidos os seguintes utentes: 2001 (18); 2002 (37); 2003 (24).

Merecem especial realce as notas e conclusões finais do relatório ao referirem o seguinte:

- “Deve ser promovida e reforçada informação e articulação entre as várias entidades envolvidas e os prestadores de cuidados;
- Para uma melhor rentabilização dos investimentos poderá contribuir a definição de uma estratégia Regional e Sub-regional, em que a actividade de telemedicina possa ou deva vir a ser integrada na regular prática clínica.
- O uso diário da telemedicina nas instituições de saúde portuguesas, por se tratar de tecnologia recente entre nós, levará o seu tempo até ser otimizada pelos técnicos, já que para além de questões de natureza tecnológica, é necessário percorrer todo um «processo de amadurecimento», dada a actual cultura e organização de trabalho das nossas instituições.
- Os utentes aceitam muito bem esta consulta e participam de forma positiva”.

Concordamos, em absoluto, com as considerações expendidas nas conclusões que acabámos de citar.

3. O *telediagnóstico* permite conferir uma especial ajuda à decisão médica, trazida por um médico a outro médico localizado à distância, a partir das informações que são transmitidas

através de um sistema telemático.

Os dois médicos envolvidos trocam os seus pontos de vista, mas o primeiro (emissor) está na situação de quem pede o conselho e o segundo de quem o dá.

Estas novas tecnologias suscitam, no entanto, novos problemas jurídicos que devem ser equacionados quer no quadro tradicional das relações entre os médicos e os doentes, quer ao nível da responsabilidade médica.

Desde logo, os doentes devem ser claramente informados de que os seus dados pessoais e a sua imagem vão ser transmitidos (cf. artigo 10.º n.º 1 da Lei 67/98), devendo ser advertidos das condições de transmissão e finalidades, por forma a aceitarem que estes dados sejam facultados a outros profissionais de saúde.

Este procedimento, que envolve a transmissão de dados por telecomunicação, obriga os estabelecimentos de saúde a tomar medidas técnicas de segurança que impeçam o acesso aos dados por pessoas não autorizadas. A utilização de linhas seguras (RIS ou linhas dedicadas) e o recurso a sistemas de encriptamento de dados deve ser assegurado, face à sensibilidade e natureza da informação processada. A compatibilidade técnica e o bom funcionamento dos equipamentos utilizados deve ser garantida ou certificada.

A prestação de cuidados de saúde com recurso à telemedicina coloca, igualmente, o acento tónico num princípio básico constante da Lei de Bases da Saúde, aprovada pela Lei n.º 48/90 de 24 de Agosto: o princípio contido na Base V que consagra «a livre escolha do médico por parte do doente». Em bom rigor, o doente vê-se confrontado perante a escolha de um profissional que não conhece – que integra a equipa que colabora no projecto de telemedicina – mas em quem pode confiar, em face das circunstâncias, insuficiências e dificuldades em poder contar com a presença de um especialista que faça um diagnóstico seguro.

4. O doente que sofreu dano na sequência de um errado diagnóstico, realizado através da utilização de sistemas de telediagnóstico, pode procurar delimitar a responsabilidade médica em função da forma como foi estabelecida a colaboração entre médicos ou da forma como

foram utilizados os aparelhos telemáticos que intervieram na decisão médica.

Deve afirmar-se que a telemedicina não pode servir de fundamento à diluição ou exclusão dos deveres profissionais e da responsabilidade médica. Por isso, será possível afirmar que os fundamentos jurídicos da responsabilidade não apresentam, em regra, especialidades em relação aos diagnósticos realizados no contexto da actividade médica prestada em equipa ou no âmbito de uma colaboração de médicos de várias especialidades.

No quadro do telediagnóstico, a diligência dos médicos deve ser apreciada em função dos papéis que cada um desempenha no estabelecimento do diagnóstico. De facto se os dois médicos, o que pede o conselho e o que o dá, trocam informações, a responsabilidade não é igual. O que pede o conselho possui a história clínica do doente, enquanto que o outro só recebe a parte seleccionada pelo colega.

Em geral, o doente dirige-se ao “médico que pede o conselho” e é dele que espera a realização de um diagnóstico adequado e da prestação de cuidados em relação à sua doença.

Para delimitar alguns aspectos de responsabilidade alguma doutrina⁽⁴⁵⁾ defende que podem ser estabelecidas cláusulas contratuais que definam as condições de atribuição de responsabilidade.

A obrigação do médico engloba, necessariamente, um completo conhecimento do manuseamento dos instrumentos utilizados. Se a captação de determinada imagem for mal efectuada, ou se as informações características de uma lesão não forem recolhidas, poderá haver lugar a um errado diagnóstico que tem na origem uma insuficiente utilização do sistema. Por esta razão será desejável que os profissionais de saúde que utilizem estas novas tecnologias tenham formação adequada, por forma a garantir que uma má utilização do sistema não origina erros de diagnóstico passíveis de responsabilidade médica.

Por uma questão de certeza e segurança em relação à tecnologia utilizada, não deverá ser negligenciada a possibilidade de haver uma entidade certificadora da qualidade destes sistemas.

⁽⁴⁵⁾ Liliane Dusserre, Henry Ducrot e François-André Allaert – “L’ Information Médicale, L’Ordinateur et la Loi”, 1996, pág. 145.

5. O sucesso da experiência de telemedicina pode ser medido em função de vários factores: número de pacientes envolvidos, em função da apreciação dos critérios custo/benefício, informação detalhada sobre o grau de participação dos médicos, percentagem de publicações científicas destes serviços, critérios que distinguem «experiências piloto» dos serviços permanentes, duração e «grau de sobrevivência» do projecto e a associação com teleserviços.

Dos contactos realizados junto dos Hospitais, ficámos com uma clara sensação de que este tipo de tecnologia está ainda longe de ser qualificada como uma experiência de sucesso. Em vários hospitais há experiências em certas especialidades clínicas que cessaram, sem que tenham sido apontadas razões objectivas.

Verifica-se que nem todos os profissionais de saúde envolvidos têm a mesma sensibilidade para a utilização destes equipamentos e que a utilização destes sistemas – por serem utilizados em horários pré-estabelecidos – nem sempre pode contar com a disponibilidade de todos os intervenientes (doente, médico que pede o conselho e médico que o dá) e que a sessão pode ficar comprometida, igualmente, por razões técnicas (v.g. de comunicação) que nem sempre são ultrapassadas.

Importa sublinhar que o recurso a estes meios deve ser institucionalizado e não deve ficar exclusivamente dependente do impulso e «carolice» de profissionais de saúde ao ponto de poder diminuir ou cessar a sua utilização se determinado profissional mais entusiasta abandona o hospital.

No que diz respeito ao enquadramento legal da telemedicina seria desejável que a Assembleia da República ponderasse a necessidade de estabelecer alguns princípios jurídicos reguladores. A utilização desta tecnologia, que se diz poder vir a ser generalizada com o objectivo de ultrapassar algumas dificuldades como a falta de médicos de determinadas especialidades em certos hospitais, deveria ser acompanhada de disposições legais que vinculassem os responsáveis a cumprir alguns dos procedimentos enunciados.

2. Os pedidos de análises clínicas e o acesso aos resultados

2. 1. Antecedentes

Em 1999 a comunicação social dava conta da violação da privacidade de alguns doentes do serviço de doenças infecciosas em dois hospitais de Lisboa, nomeadamente em relação ao pedido de análises clínicas de doentes portadores de HIV.

Feitas as diligências no respectivo processo verificou-se que, no âmbito da realização de exames auxiliares de diagnóstico (pedido de análises) era "preenchido um formulário no qual consta o nome, a idade, o n.º de processo, o diagnóstico (cf. os impressos juntos ao processo - HIV) e serviço de origem, bem como as análises pedidas".

Era um funcionário administrativo (da secretaria) que marcava as análises⁽⁴⁶⁾ mediante a entrega do pedido no centro de "triagem". Esse funcionário administrativo introduzia os dados em suporte informático: dados administrativos e diagnóstico quando preenchido, bem como os elementos relativos à identificação da amostra.

A CNPD fez uma apreciação da forma como eram tratados os dados, na Deliberação n.º 23/99-A, de 2 de Julho⁽⁴⁷⁾, tendo sugerido algumas alterações aos procedimentos internos de tratamento de dados dos doentes. Em particular, foram impostas novas metodologias relativas à circulação da informação. Salientam-se, nessa deliberação, as seguintes conclusões:

- a) A «partilha da informação clínica» ou a cedência de dados de saúde no âmbito do estabelecimento hospitalar deve ser feita na estrita medida do necessário à prestação de cuidados de saúde, ou seja, os dados de saúde (vg. o diagnóstico) só deverão ser transmitidos quando se revelem necessários à prestação de cuidados de saúde ao utente.

⁽⁴⁶⁾ Constatou-se, na altura, que o diagnóstico de HIV era um dos motivos determinantes para a "prioridade" na realização das análises.

⁽⁴⁷⁾ In Relatório da CNPD de 1999, pág. 99.

- b) A inscrição do diagnóstico no pedido de análises - com acesso por parte de funcionários administrativos e pessoal que procede à colheita de sangue - viola a privacidade dos utentes e põe em causa a confiança que deve ser estabelecida na relação médico doente (cf., também, a Base XVI n.º 1 al. c) e d) da Lei de Bases da Saúde aprovada pela Lei n.º 48/90, de 24 de Agosto). Todos os procedimentos vigentes que permitam o acesso aos dados de diagnóstico por parte destes funcionários administrativos devem ser imediatamente suspensos.
- c) Muito embora se considere que a generalidade dos pedidos de análise não necessita da especificação do diagnóstico admite-se que, em casos pontuais, a especificação de um “diagnóstico possível” possa ser útil para efeito da elaboração do diagnóstico definitivo. Neste caso, a «partilha da informação» é feita no interesse do doente e para efeito de diagnóstico médico.
- d) No caso referido no ponto anterior haverá legitimidade, nos termos do artigo 7.º n.º 4 da Lei 67/98, para a “comunicação” da informação ao médico analista. Porém, o Hospital deveria estabelecer uma metodologia (vg. utilização de envelope ou carta fechada) que impossibilite o acesso ao diagnóstico por parte de funcionários administrativos ou outros funcionários a quem está vedado o acesso àquela informação.

Na sequência desta deliberação verificou-se que num dos hospitais foram alterados alguns procedimentos internos. Em especial, o impresso relativo ao pedido de análises de qualquer serviço do Hospital – quando tinha inscrito o diagnóstico do paciente – deveria ser “agrafado” por forma a garantir a impossibilidade de acesso àquela informação por parte de funcionários administrativos e de outros funcionários do serviço de análises clínicas.

Com o decurso do tempo tal procedimento “caiu no esquecimento” e constatou-se que aquele procedimento só era mantido no Serviço de Doenças Infecciosas. Ora, perante tal situação não fazia sentido “ocultar” o diagnóstico uma vez que o facto de o pedido vir “agrafado” era indicador de suspeita de HIV e, conseqüentemente, gerador de discriminação.

Perante tal constatação a CNPD pronunciou-se novamente sobre a forma de assegurar a confidencialidade da informação de saúde inserta nos pedidos de análises – Deliberação n.º 34/2002, de 26 de Fevereiro⁽⁴⁸⁾ – reafirmando, mais uma vez que:

- a) *Todos os serviços do Hospital* devem passar a “agrafar” os pedidos de análises, por forma a que não seja possível visualizar o diagnóstico do doente;
- b) Nem os funcionários administrativos nem os funcionários que realizam as colheitas estão autorizados a “desagrafar” os pedidos, cabendo ao profissional responsável pela realização da análise (vg. o analista) proceder à remoção do “agrafe”;
- c) A Direcção do Hospital deverá fazer uma ordem de serviço interna que imponha este procedimento, adoptando as medidas adequadas em relação às pessoas que violarem as suas ordens;
- d) A Direcção do Hospital deverá alterar os formulários que não permitam, na prática, ocultar o diagnóstico.

A metodologia sugerida, que mereceu o acordo da Direcção do Hospital, tinha em vista contribuir para assegurar a confidencialidade da informação clínica e evitar a discriminação dos doentes.

2.2. A situação actual

1. Num dos Hospitais visitados verificou-se que a generalidade dos pedidos de análises continuam a ser remetidos ao Serviço de Patologia Clínica *em suporte de papel* sendo os dados administrativos e o «diagnóstico possível» acessíveis ao funcionário administrativo que insere os dados na aplicação informática deste Serviço. Os poucos pedidos que vêm «agrafados» são oriundos do Serviço de Infecçiology. Mais uma vez se constata a total

⁽⁴⁸⁾ In Relatório da CNPD de 2002.

ineficiência do sistema adoptado, facto que pode comprometer a relação de confiança entre o médico e o doente.

Mas, embora não tenham chegado à CNPD queixas em relação a outros hospitais, verifica-se que o risco de discriminação é potencial na medida em que – em termos gerais – os procedimentos são similares. A confirmar esse risco de discriminação basta referir ter sido constatado num hospital, sem que haja razão objectiva ou apresentada qualquer justificação, a existência de uma prática institucionalizada de dar prioridade na realização de análises clínicas a pessoas grávidas e cidadãos portadores de HIV.

2. Em todos os hospitais visitados (38) foram verificadas 62 aplicações informáticas – 61 em rede e 1 em computador isolado⁽⁴⁹⁾ – destinadas à gestão de análises clínicas, nomeadamente nos Serviços de Patologia Clínica, de Imunohemoterapia e Serviço de Sangue. Um hospital não dispõe de aplicação informática para gestão da informação de pedidos de resultados. Naqueles tratamentos automatizados, apenas 3 se limitavam a tratar dados administrativos procedendo os restantes (59), também, à gestão de informação clínica.

Em relação aos tratamentos que fazem registo de informação clínica (59) há 45 aplicações que permitem a inserção do «diagnóstico possível»⁽⁵⁰⁾, não possuindo as restantes qualquer campo para o registo desta informação. Constata-se que em 39 tratamentos é registado, neste momento, o «*diagnóstico possível*». Verifica-se, em relação à totalidade dos pedidos de análises (63), que em 59 serviços os pedidos são ainda feitos em suporte de papel. Em 3 hospitais os pedidos de análise são feitos *on line* (pela rede do Hospital) e num caso (Serviço de Sangue) os dados são inseridos directamente e *on line* pelo médico, sem utilização de suportes de papel. Em 5 hospitais há *alguns serviços* que fazem os pedidos de análises através da rede (com especial incidência nos Serviços de Urgência e na Unidade de Cuidados Intensivos). Um hospital, apesar de fazer os pedidos através da rede, continua a enviar os formulários em papel ao serviço de patologia clínica.

⁽⁴⁹⁾ Num Hospital existe, em simultâneo, uma ficha em suporte de papel para cada doente.

⁽⁵⁰⁾ Em 6 casos o campo para registo do «diagnóstico possível» não é preenchido.

Em relação aos pedidos em suporte de papel verifica-se que não há qualquer precaução no que se refere à preservação da confidencialidade do «diagnóstico possível» uma vez que esses pedidos circulam no interior do Hospital sem qualquer medida de segurança (v.g. em carta fechada). A informação dele constante continua acessível a qualquer funcionário do Serviço, nomeadamente a funcionários (administrativos) que não precisam de ter acesso ao «diagnóstico possível» para exercerem as suas funções.

Tal como tem entendido a CNPD (cf. a citada Deliberação n.º 23-A/99), a circulação da informação deve «obedecer a um princípio de “confidencialidade necessária” em que serão determinantes para definir o “âmbito do segredo” o interesse do doente, a natureza da informação e os reflexos que a sua divulgação traz para a sua privacidade». Por isso, impõe-se que a informação relativa ao diagnóstico só seja fornecida «aos profissionais de saúde que, por força das funções que desempenham, dela necessitam para a realização das prestações de saúde»⁽⁵¹⁾.

Neste contexto, e uma vez que os dados administrativos e o pedido de análises são introduzidos nas aplicações por funcionários administrativos, confirmaram-se grande parte das constatações já evidenciadas na Deliberação n.º 23-A/99. Em 45 aplicações (cerca de 72,5% em relação ao total) o funcionário administrativo tem acesso ao diagnóstico possível, registando-o na respectiva aplicação em 39 serviços.

3. As aplicações informáticas, em geral concebidas por empresas privadas, fazem a separação lógica entre dados administrativos e dados de saúde, adoptando *medidas de segurança adequadas*. Assim, constatou-se o seguinte:

- a) 69 aplicações possuem *password*, tendo-se verificado que duas não tinham *password*;
- b) Em 60 casos eram feitos *backups*, não sendo feitas cópias de segurança em 2 casos. Nas situações em que foi possível apurar com rigor a periodicidade da realização de *backups*

⁽⁵¹⁾ Cf. neste sentido “Vie Privée et Droits de L’Homme », Actes du Troisième Colloque International sur la Convention Européenne des Droits de l’Homme, 30 de Setembro a 3 de Outubro de 1970, pág. 218 e 219.

deve considerar-se essa periodicidade como adequada. Ou seja, realizam-se cópias de segurança diária em 43 aplicações, sendo feitas de 3 em 3 dias em 3 casos e havendo duas situações com realização de cópias de segurança semanal. Em 11 casos não foi dada informação e num caso foi referido que os *backups* apenas são realizados “quando o disco está cheio”.

4. Destas aplicações verifica-se que apenas 14 tratamentos se encontram notificadas à CNPD, sendo de salientar que cerca de 77% do total destes tratamentos (49) não foram notificados. Em 11 destas aplicações (10 relativas a Serviços de Sangue) procede-se ao tratamento do dado «raça». Tal percentagem de incumprimentos da lei, sabendo-se que em geral os hospitais têm consciência da obrigatoriedade de notificação dos tratamentos, não deixa de ser preocupante e reveladora da falta de cuidado no cumprimento da lei.

5. Nas 13 aplicações de Serviço de Sangue, para além dos dados de saúde e da raça, é feito o tratamento dos seguintes dados pessoais sensíveis: droga/toxicod dependência (em 5 casos); HIV (5); hábitos sexuais (5); parceiros (5); prostituição (5); comportamento de risco (1); hábitos alcoólicos (2). Estes dados sensíveis são também acessíveis, em 6 hospitais, a funcionários administrativos.

Em face da natureza dos dados, e tendo em atenção o disposto nos artigos 7.º n.º 1 e 2 e 28.º n.º 1 alínea a) da Lei 67/98, de 26 de Outubro, estes tratamentos devem ser objecto, necessariamente, de controlo prévio da CNPD. Justifica-se que, em face da extrema sensibilidade da informação tratada, a CNPD se deva pronunciar em relação à necessidade e imprescindibilidade do tratamento desta informação. Aliás, deve anotar-se que a CNPD tem sido extremamente exigente na justificação do tratamento do dado raça e já se pronunciou de forma muito restritiva em relação ao tratamento de dados desta natureza no contexto dos «serviços de sangue»⁽⁵²⁾.

⁽⁵²⁾ Em relação ao tratamento realizado pelo Instituto Português de Sangue a Comissão teve oportunidade de considerar, ainda no domínio da lei 10/91, que não havia necessidade de «proceder ao registo específico da

O controlo prévio visa, igualmente, garantir que aos titulares seja dado o direito de informação de forma clara para assegurar que o tratamento seja realizado com observância das «condições de legitimidade» legalmente estabelecidas no artigo 7.º n.º 2 da Lei 67/98. Isto é, mediante «consentimento expresso» para o tratamento daqueles dados, consentimento esse que deve ser dado de forma “livre, específica e informada” (cf. artigo 1.º alínea h) da Lei 67/98). Nenhum hospital apresentou qualquer elemento que permitisse apurar a existência de consentimento para o tratamento daqueles dados.

Ora o que se verifica em relação a estas aplicações é que apenas 1 se encontra notificada. Mas, apesar de tratar a raça, a toxicodependência, HIV, hábitos sexuais, parceiros e «prostituição», não consta do pedido de notificação entregue na CNPD qualquer referência ao tratamento destes dados. O tratamento encontra-se autorizado, sem que a CNPD se tenha pronunciado em relação ao tratamento destas categorias de dados por omissão de informação da parte do hospital responsável.

A falta de notificação inviabiliza o controlo prévio, em face da natureza dos dados, no que diz respeito a estes tratamentos. A omissão de notificação em situações deste tipo – ainda que seja negligente – reveste-se de especial gravidade, facto que levou o artigo 37.º n.º 2 da Lei 67/98 a cominar com a agravação da coima para o dobro dos seus limites.

6. No que diz respeito ao *direito de informação* – que deve ser assegurado nos termos do artigo 10.º da Lei 67/98 – verifica-se, tal como foi referido supra, a inexistência de

"homossexualidade ou comportamento sexual promíscuo", de "parceiros sexuais de indivíduos em risco" ou de "toxicodependência"» na medida em que a constatação de tais factos sempre pode ser reconduzido «a "conclusões clínicas" de carácter geral já previstas nas respectivas Tabelas - vg. "não compatível com a dádiva" (S001), "recusa" (S330) ou com outro descritivo - permitindo obter os mesmos efeitos ao nível da "qualidade do sangue", sem registar referências susceptíveis de discriminação e violação da privacidade» (cf. Parecer n.º 13/95, de 10 de Outubro – 2.º Relatório, pág. 276). Também a Deliberação n.º 23-A/99, de 2 de Junho (Relatório de 1999, pág. 99) considerou que «os dados pessoais que referenciam um cidadão como "homossexual, bissexual, prostituta, heterossexual com múltiplas parceiras, criança filha de prostituta, de parceira bissexual, de parceira heterossexual com múltiplos parceiros" se enquadram no âmbito da sua "vida privada" (art. 35.º da CRP e art. 7.º n.º 1 da Lei 67/98). O tratamento daqueles dados só pode ser feito *quando o seu titular o consentir de forma expressa* e desde que as fichas clínicas sejam guardadas em sala que permita um controlo efectivo da entrada nas instalações onde as mesmas estão arquivadas».

procedimentos ou preocupações para assegurar aquele direito. Em 60 tratamentos (cerca de 95,2%) não se apurou que existisse qualquer mecanismo que tivesse em vista informar os titulares sobre a realização de tratamento de dados, especificação de finalidades⁽⁵³⁾ ou destinatários das informações.

Apenas 3 serviços (serviços de sangue) afirmam que asseguram o direito de informação. Num dos casos pressupõem a existência de direito de informação pelo simples facto de os dados pessoais serem introduzidos *on line*, na presença do titular. Nos outros dois casos informam os responsáveis que o direito de informação é assegurado por escrito em documento que é entregue ao dador de sangue. Conforme vimos supra, o teor do texto inserto nos referidos documentos não satisfaz os pressupostos legais relativos ao direito de informação.

7. No que diz respeito ao **acesso aos resultados** verifica-se que, em relação às 62 aplicações analisadas, há 53 casos em que os resultados são *impressos em papel*, podendo os resultados encaminhados da seguinte forma (resposta múltipla):

- ❑ Entrega ao doente – 6
- ❑ Enviados ao médico/serviço requisitante – 43⁽⁵⁴⁾
- ❑ Impressão remota no serviço – 5
- ❑ Arquivados no próprio serviço – 4

Em 31 casos já foram estabelecidos mecanismos de consulta dos resultados em tempo real. Isto não significa que todos os serviços do hospital possam consultar *on line* os resultados das análises, podendo acontecer que essa consulta seja disponibilizada para alguns serviços. Interessa salientar que as formas de consulta podem ser diversificadas, em função das condições técnicas disponíveis no hospital:

⁽⁵³⁾ Não se pode esquecer que, em muitos casos, os dados são utilizados com finalidade de investigação científica.

⁽⁵⁴⁾ Num hospital foi informado que os resultados do HIV/SIDA são remetidos em carta fechada.

- ❑ O médico do hospital que dispõe de *password* adequada pode **sempre** consultar as análises através da rede⁽⁵⁵⁾ – 8;
- ❑ Só determinados serviços do hospital podem consultar os resultados (v.g. Urgência, UCI) – 12;
- ❑ Os resultados são enviados pela rede ao serviço requisitante – 5;
- ❑ As análises são apenas acessíveis no próprio serviço (Serviço de Sangue) – 7

8. No que diz respeito aos *prazos de conservação* dos dados verificou-se que não foram estabelecidos prazos de conservação da informação. Em apenas 2 Serviços de Sangue se encontra estabelecido um prazo de conservação, correspondente ao prazo legalmente fixado (50 anos).

Nos restantes casos (61) os dados são guardados de forma «permanente», ou seja, desde o início da exploração da respectiva aplicação.

Este procedimento viola os princípios de protecção de dados segundo os quais «os dados devem ser exactos e, se necessário, actualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou rectificados os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente» (artigo 5.º n.º 1 al. d) da Lei 67/98).

2. 3. A solução preconizada para reforçar a confidencialidade

A generalidade dos hospitais possui, hoje, aplicações informáticas para gestão da informação relativa a análises clínicas. Verifica-se, porém, que os procedimentos actualmente adoptados na grande maioria dos hospitais devem ser objecto de ajustamento por forma a melhorar a confidencialidade em relação aos dados tratados.

⁽⁵⁵⁾ Em relação a utentes com HIV os resultados não são disponibilizados através da rede.

Constata-se que os vários serviços dos hospitais *requisitam análises clínicas* em suporte de papel, muitas vezes circulando internamente sem o mínimo cuidado e permitindo aos funcionários administrativos – que fazem as marcações das análises – conhecer o «diagnóstico possível», o qual vem anotado nas respectivas requisições. Em determinadas doenças discriminatórias – v.g. SIDA/HIV, hepatite, doenças do foro sexual ou oncológico – tem-se verificado que o acesso a esta informação por aqueles profissionais suscita algumas objecções por parte dos cidadãos envolvidos, sentindo que estão a ser discriminados em função da forma como são atendidos. Acresce, por outro lado, que o acesso ao diagnóstico por parte daqueles profissionais (funcionários administrativos) não se apresenta como necessário ao desempenho das suas funções.

No momento em que as redes hospitalares cobrem, na generalidade dos casos, todos os serviços dos hospitais e não são excessivamente dispendiosas ferramentas (nalguns casos já disponíveis) que viabilizam os pedidos em tempo real através da rede, importa que os hospitais dêem prioridade à adopção das medidas técnicas necessárias que assegurem a requisição *on line* dos pedidos de análises clínicas⁽⁵⁶⁾. Esta medida contribuirá, de forma decisiva, para reforçar a confidencialidade em relação à informação clínica e de garantias de que o acesso àquela informação é reservado aos profissionais de saúde que dela necessitem para o exercício das suas funções.

Pela mesma ordem de fundamentos justifica-se que os resultados das análises possam ser consultados *on line* pelos serviços requisitantes e estejam acessíveis, em tempo real, a alguns serviços para obviar à requisição de exames desnecessários.

Desde que adoptadas as medidas de segurança adequadas pensamos que estas modificações contribuirão para reforçar a confidencialidade da informação clínica. Essas modificações, que pressupõem um melhor aproveitamento das novas tecnologias, não apresentam problemas

⁽⁵⁶⁾ Também o relatório a que já nos referimos, realizado pela empresa World Software Services, coloca o acento tónico na necessidade de “implementar uma intranet e ferramentas de gestão documental”. Advoga, por isso, a adopção de “sistemas de partilha de dados e aplicações entre os diversos profissionais” como forma de «aumentar a eficiência dos processos de trabalho» e de permitir uma «uniformização de valores ao longo da instituição, a disseminação de informação e directrizes de trabalho e o desenvolvimento contínuo das aptidões e conhecimentos dos profissionais».

jurídicos dignos de realce. Pelo contrário, permitem o estabelecimento de «níveis de acesso» em função da natureza da informação tratada, conferindo “medidas de segurança reforçada” e evitando o acesso indevido por pessoas não autorizadas.

A CNPD espera que, *no decurso dos próximos 6 meses*, seja feito um esforço substancial no sentido de acelerar o processamento desta informação em tempo real, sob pena de poder vir a tomar medidas coercivas para conseguir garantir a efectiva confidencialidade da informação e evitar a discriminação dos titulares dos dados. Em particular, sabendo-se que o SAM dispõe de ferramenta que permite assegurar o cumprimento destes objectivos, lança a CNPD um desafio ao IGIF para, na medida do possível, colocar este objectivo na sua agenda de prioridades. Esta alteração melhorará, de forma significativa, a confidencialidade da informação no interior do hospital.

3. Arquivo Clínico

1. À excepção do Hospital dos SAMS – que gere a informação através de um *processo clínico informatizado* – todos os outros hospitais possuem uma ficha clínica em suporte de papel da qual consta a história clínica do doente. Verifica-se que 32 hospitais têm um arquivo centralizado, havendo 6 que têm arquivos específicos para determinadas especialidades (v.g. psiquiatria, oncologia, gestão de doentes, internamento, genética) e que funcionam de forma autónoma. Isto é, o mesmo doente pode ter dois processos clínicos autónomos no caso de ter sido assistido em duas especialidades que têm arquivos próprios.

Há 3 hospitais onde não existe qualquer aplicação informática para gestão da ficha clínica. Foram analisadas 37 aplicações para a gestão da ficha clínica. Destas aplicações, em 67,5% dos casos apenas são processados dados administrativos para localização da ficha clínica, em 32,5% das situações a aplicação processa informação administrativa e clínica. De entre essas aplicações há uma que não está dotada de *password* nem faz processamento de *backups*.

2. Verificou-se que 7 hospitais facultaram à CNPD regulamentos referentes ao Arquivo Clínico⁽⁵⁷⁾. Alcança-se do teor dos vários regulamentos que o arquivo clínico é a Unidade Administrativa responsável pela recepção, organização e controlo do circuito, guarda/conservação e localização ou empréstimo de documentos referentes ao estudo, diagnóstico e tratamento de doentes/utentes do hospital.

Em geral compete ao arquivo, nomeadamente:

- Receber toda a documentação clínica referente aos vários episódios de diagnóstico e tratamento de doentes no hospital, organizá-la em Processo Clínico Único e preservá-la de forma a que esteja disponível para consulta quando necessário.
- Manter actualizado o registo informático dos elementos relativos ao movimento de processos clínicos, garantindo a eficaz localização e consulta dos mesmos;
- Garantir adequada informação sobre os antecedentes clínicos de doentes com o objectivo prestação de cuidados de saúde ou para o caso de novo recurso ao Hospital;
- *Manter todos os processos clínicos e radiológicos arquivados de acordo com a respectiva numeração sequencial;*
- *Arquivar toda a documentação e/ou exames complementares de diagnóstico e terapêuticas dos doentes;*
- Suportar estudos científicos devidamente autorizados;
- Suportar elaboração de *curricula* do pessoal técnico hospitalar;
- Constituir fundo documental que permita responder a solicitações de informação dos tribunais ou outras partes legalmente interessadas.

Existem, nos diferentes regulamentos, regras diversas sobre o acesso e consulta dos documentos em arquivo.

⁽⁵⁷⁾ Hospital do Barlavento Algarvio, Garcia de Orta, Fernando Fonseca, Centro Hospitalar Funchal, Hospital de Santarém, Hospital de Santa Cruz e Hospital de S. António.

Se bem que, em geral, os regulamentos refiram que a consulta do processo clínico para fins diversos da prestação de cuidados é feita no próprio arquivo ou local próprio para o efeito, no respeito pelas finalidades do tratamento da informação e pelo princípio da confidencialidade dos dados clínicos, a verdade é que, na prática, o processo clínico pode sair do arquivo.

Admite um regulamento que, mediante autorização do Director Clínico, os médicos estranhos à instituição podem consultar o processo clínico, mediante requisição e em sala própria no Arquivo clínico⁽⁵⁸⁾.

Os regulamentos podem estabelecer prazos limite para o «levantamento» do processo do arquivo: não poderá ser facultado o levantamento de qualquer elemento do processo clínico do respectivo arquivo por períodos superiores a 10 dias úteis, salvo autorização especial a conceder caso a caso, em face das razões invocadas.

Em face da reconhecida vulnerabilidade e do fácil manuseamento dos suportes em papel, os regulamentos alertam para a necessidade se evitar que «os processos clínicos estejam ao alcance, quer dos próprios doentes a que respeitam, quer dos respectivos familiares, e/ou dos visitantes».

Mas, tal como foi referido na Deliberação n.º 100/2004, de 13 de Julho, “o dossier clínico em suporte de papel não confere as mesmas garantias de confidencialidade que podem ser asseguradas com a informatização do processo clínico. Muito embora o regulamento denote uma preocupação em limitar o acesso ao processo clínico, estamos certos que a sua informatização/digitalização irá responder às preocupações de preservação da confidencialidade”.

3. Em relação à questão de saber quem pode pedir as fichas clínicas ao arquivo (resposta múltipla), foram obtidas as seguintes respostas:

- Qualquer médico do hospital – 30
- O médico que tem consulta marcada – 36
- Qualquer funcionário administrativo – 1

⁽⁵⁸⁾ Hospital de Santarém

- Qualquer profissional de saúde ligado à equipa – 2
- Qualquer funcionário do Hospital – 1
- O médico para investigação científica⁽⁵⁹⁾ – 33

Um dos aspectos que tem preocupado a CNPD e que tem sido objecto de dúvidas em relação à preservação da confidencialidade prende-se com a forma como é manuseado o processo clínico. Desde logo, é relevante conhecer quem faz o transporte da ficha clínica dos arquivos para o respectivo serviço. Neste domínio foi possível apurar os seguintes dados (resposta múltipla):

- Funcionário do arquivo – 19
- Funcionário administrativo – 14
- Auxiliar de acção médica (funcionário de consulta externa) - 7
- Secretária de Unidade – 1
- Auxiliar de apoio e vigilância – 1
- Funcionário do atendimento – 1
- Funcionário administrativo de gestão de doentes – 1

A confidencialidade da informação também pode ser preservada em função da forma como circula o processo clínico no interior do hospital. Neste domínio foi possível apurar o seguinte (resposta múltipla):

- Em pasta (que pode ser aberta) – 13
- Em «lotes» de acordo com os serviços ou consultas⁽⁶⁰⁾ – 28
- Em recipiente fechado – 1
- Em mão – 1

⁽⁵⁹⁾ Em dois hospitais o acesso para investigação depende da autorização do director clínico. Em 2 hospitais a autorização da direcção clínica deve ser precedida da necessária autorização da Comissão de Ética. Um hospital exige a avaliação da parte do director de serviço onde o médico se encontra inserido. Dois hospitais referiram que não tiveram qualquer pedido de consulta de processo clínico para fins de investigação científica.

⁽⁶⁰⁾ É a forma mais usual. Os processos clínicos são agrupados em função dos serviços ou das consultas, sendo enviados por conjuntos («lotes») podendo ser colocados elásticos ou outros mecanismos de ordenação.

- Em envelope – 1
- SAM'S - «dossier clínico informatizado»

4. Alguns regulamentos referem, de forma expressa, que é «proibida a saída de qualquer processo clínico para fora do edifício, constituindo a preterição desta regra fundamento para o procedimento disciplinar»⁽⁶¹⁾.

Mas, não deixa de ser curiosa a reacção das pessoas inquiridas quando se pretende saber, de forma singela, se o «processo clínico pode sair do hospital». À excepção de um caso, em que se admite essa possibilidade, a reacção imediata é sempre a mesma (36 hospitais): «*O processo clínico não pode sair do hospital*».

Porém, algumas das pessoas contactadas – sem se pronunciarem abertamente sobre a situação real – fazem crer que aquela resposta peremptória tem algo de enganador uma vez que, na prática, o percurso da ficha clínica pode fugir ao controlo dos responsáveis do arquivo. Como é óbvio, se o processo clínico é entregue ao médico não é crível que os funcionários do arquivo fiscalizem a actuação dos médicos ou investigadores no que diz respeito à localização do processo clínico que lhe foi confiado.

A comprovar tal suspeita que nos ocorreu, basta citar alguns comentários que ouvimos no momento em que fizemos tal pergunta: “não há controlo”!... “Na prática acontece e não podemos garantir que não aconteça”... “Por regra, não! Mas há alguns casos em que é possível sair”... “Às vezes sai!”... “Mas pode sair, porque não controlamos!”... “Os médicos levam o processo clínico⁽⁶²⁾ por muito tempo e por vezes não o localizamos!”... “Têm meses o processo em casa!”... Em face destes comentários somos levados a admitir que não há garantias efectivas de que o processo clínico não saia do hospital, correndo-se o risco de não se encontrar disponível, nomeadamente, quando o doente se possa dirigir ao hospital com o objectivo de ser submetido à prestação de cuidados de saúde.

⁽⁶¹⁾ Hospital Fernando Fonseca e de Santa Cruz.

⁽⁶²⁾ Em geral, para fins de investigação científica ou elaboração de relatórios médicos.

Na mesma linha de pensamento, deve ser impossibilitado o acesso à informação clínica por parte dos utilizadores (médicos ou enfermeiros) através de postos de trabalho externos ao Hospital. Sendo o acesso ao *dossier* clínico justificado no âmbito do diagnóstico ou prestação de cuidados de saúde, não deverá ser permitidos aos utilizadores o acesso directo através de terminais colocados no exterior do Hospital.

5. Do que ficou exposto, consideramos que o facto de o processo clínico se encontrar em suporte de papel é motivo bastante para considerar que, por mais esforços que sejam feitos, existem sempre riscos de a informação clínica ser acessível por terceiros não autorizados. O processo clínico em papel encontra-se, por natureza, exposto à curiosidade geral – quer no próprio arquivo, quer nos serviços por onde circula – não havendo mecanismos eficazes que assegurem a impossibilidade de devassa. A CNPD considera que só os suportes automatizados dotados das necessárias seguranças – *passwords* com «perfis de utilizadores» bem definidos, separação lógica entre dados administrativos e de saúde – podem conferir a necessária confidencialidade à informação clínica dos doentes. Enquanto isso não acontecer ninguém está em condições de garantir a inexistência de acessos indevidos por pessoas não autorizadas⁽⁶³⁾. Porém, quaisquer tentativas para a generalização do *dossier* clínico automatizado – quer através da informatização global do processo clínico, quer da digitalização da ficha clínica – depara com obstáculos de ordem prática em relação aos suportes. Têm-se colocado dificuldades em relação à automatização da ficha clínica, apresentando-se como objecção fundamental a existência de problemas jurídicos relativos à força probatória dos suportes

⁽⁶³⁾ Numa perspectiva de conferir «elevada disponibilidade, rapidez de acesso e segurança» em relação à informação clínica a World Software Services propõe, no mesmo contexto, a implementação no Hospital de um «Arquivo Clínico Electrónico e um Arquivo de Imagem Médica Electrónica» que evoluirá gradualmente à medida que o processo de digitalização do histórico puder responder. Nesse relatório são evidenciadas, com particular rigor, as vantagens dos arquivos digitais em relação aos suportes de papel.

automatizados⁽⁶⁴⁾. Encontra-se enraizada a ideia de que só os suportes de papel podem fazer prova, nomeadamente quando solicitados pelo Tribunal.

Para além de termos dúvidas em relação a esta objecção – já que muitos diagnósticos (v.g. meios auxiliares de diagnóstico) estão hoje suportados em documentos produzidos pelo próprio computador (dados esses que podem ser consultados no écran ou impressos) – pensamos que, à semelhança do que acontece com outras realidades da actividade económica (registos e notariado, contribuições impostos, informação contabilística), é necessário que se tomem medidas legislativas clarificadoras que confirmem força probatória similar aos suportes automatizados utilizados em ambiente hospitalar. Esta solução dissiparia quaisquer dúvidas que têm vindo a ser colocadas e que são um obstáculo relevante à institucionalização de medidas – que muitos hospitais pretendem e advogam – que visam a automatização do processo clínico.

Deve anotar-se, finalmente, que tanto a prova constante da ficha clínica como aquela que é produzida pelo computador com intervenção humana será apreciada livremente pelo juiz.

Aliás, nem sequer podem suscitar-se dúvidas sobre a “falsificação” de fichas clínicas uma vez que, na prática, é bem mais difícil viciar uma ficha clínica que foi digitalizada do que modificar uma ficha clínica em suporte de papel. Uma ficha clínica em suporte de papel pode ser substituída e escrita de novo, enquanto a ficha clínica digitalizada pode ser insusceptível de alteração se forem utilizadas tecnologias adequadas similares às certificações vigentes em matéria de assinatura digital.

Os suportes automatizados ou a digitalização das fichas clínicas oferecem, sem dúvida, garantias acrescidas em relação à confidencialidade da informação contida na ficha clínica, razão pela qual advogamos a substituição gradual dos suportes, acompanhada das alterações

⁽⁶⁴⁾ O regulamento do Hospital do Barlavento Algarvio dispõe, a este propósito, o seguinte: “Quando, na conservação de elementos clínicos for utilizado suporte diferente do papel, nomeadamente por microfilme ou suporte informático, os originais serão conservados em arquivo morto até que seja publicada legislação que permita a sua destruição».

legislativas necessárias. Esta via é a única que deve ser adoptada para garantir a confidencialidade efectiva da informação.

Alguns hospitais referiram ter em estudo projectos de digitalização dos seus arquivos como forma de resolver problemas práticos de grande complexidade, quer no domínio da gestão/localização rápida do *dossier* clínico, quer em relação à gestão de espaços nos Hospitais. No entanto, as suas iniciativas esbarram na dúvida e entraves que lhes têm sido colocados em relação à possibilidade de destruição dos suportes de papel. Efectivamente, as suas iniciativas só serão rentáveis se os suportes de papel puderem, gradualmente, ser substituídas por suportes automatizados.

Essa deve ser, na nossa óptica, uma prioridade a considerar pelo Ministério da Saúde.

6. Um outro aspecto que tem suscitado algumas dificuldades nos hospitais prende-se com a apreciação de pedidos de acesso por parte de terceiros (seguradoras, familiares, tribunais, segurança social) ao processo clínico.

Em termos de procedimentos para apreciação dos pedidos afigura-se-nos que foram adoptados mecanismos que conferem particular rigor à decisão a tomar uma vez que são chamados a intervir profissionais com especial sensibilidade em matéria de preservação da confidencialidade. Efectivamente, na generalidade dos hospitais tal decisão passa sempre pelo director clínico (36 casos), admitindo-se em situações particulares que tal decisão possa ser precedida de parecer dos serviços jurídicos ou do director do serviço. Há 7 situações onde a decisão final cabe à Direcção do Hospital.

A generalidade dos hospitais, que se queixou da falta de legislação sobre acesso de terceiros aos dados de saúde, saudou e evidenciou o especial contributo que a Deliberação da CNPD 51/2001, de 3 de Julho, tem tido na apreciação da generalidade dos pedidos formulados. A verdade é que a CNPD, embora tenha feito um esforço no sentido de abarcar nessa deliberação as situações mais frequentes, continua a ser confrontada com sucessivos pedidos de acesso em face da falta de disposições legais que definam as situações em que será admissível o acesso,

por parte de terceiros, a dados constantes do processo clínico. Em 2001 e 2002 deram entrada, respectivamente, 197 e 109 pedidos de acesso⁽⁶⁵⁾, em 2003 foram registados 61 pedidos e até 30 de Setembro de 2004 foram formulados 35 pedidos.

Estes pedidos continuam a ter um peso significativo na actividade da CNPD, sendo desejável que se considere como prioridade legislativa a adopção de disposições legais relativas ao «acesso à informação clínica» no interior dos estabelecimentos de saúde.

Tal opção acabaria por clarificar algumas soluções que têm vindo a ser preconizadas pela CNPD, muito questionadas por algumas entidades, e que não foi possível à Comissão apurar que reflexos têm tido em termos de prejuízo para os cidadãos. Estamos a referir-nos, em concreto, ao acesso ao processo clínico por parte de Companhias de Seguros nas situações em celebraram contratos de seguro de vida. A CNPD tem entendido que – não havendo cláusula contratual⁽⁶⁶⁾ ou consentimento expresso e informado dos titulares dos dados para acesso ao seu processo clínico após a sua morte – o acesso só é possível com o consentimento do doente.

Há situações que, ao que referem os beneficiários dos seguros, a indemnização só é paga quando é facultado o acesso ao processo clínico do segurado. Sendo a CNPD muito restritiva em relação ao acesso ao processo clínico – porque se trata de informação da vida privada – importa saber se este entendimento, que tem suporte na lei (artigo 7.º n.º 2 da Lei 67/98) não se traduz em prejuízo para os beneficiários dos seguros.

Deste modo, e à semelhança do que acontece noutros países (v.g. França e Bélgica), considera a CNPD que a Assembleia da República deveria legislar sobre as condições em que os hospitais ou os médicos poderiam facultar o acesso a dados de saúde por parte de terceiros (em particular Companhias de Seguros) após a morte dos titulares dos dados.

⁽⁶⁵⁾ Vejam-se os dados estatísticos do Relatório da CNPD de 2001 e 2002.

⁽⁶⁶⁾ Muitas cláusulas contratuais apresentam-se como sendo de validade duvidosa. A verdade é que não compete à CNPD apreciar a validade de certas cláusulas insertas nos contratos de seguro.

4. Caminhar para um *dossier* clínico informatizado

1. Para além dos aspectos relativos à privacidade e confidencialidade da informação clínica, o tratamento de dados de saúde pode ser abordado noutras perspectivas.

A Decisão n.º 1786/2002/CE do Parlamento Europeu e do Conselho de 23 de Setembro de 2002⁽⁶⁷⁾ aprovou um «programa de acção comunitário no domínio da saúde pública (2003-2008)». Este programa tem em vista, entre outras finalidades, “melhorar a informação e os conhecimentos com vista ao desenvolvimento da saúde pública” (artigo 2.º n.º 2 alínea a). Com vista à execução deste programa dispõe o artigo 5.º n.º 4 que a Comissão, em estreita cooperação com os Estados-Membros, “procura garantir a compatibilidade dos dados e informações e, sempre que possível, a compatibilidade e interoperacionalidade dos sistemas e redes de intercâmbio de dados e informações em matéria de saúde”. A execução deste programa deve assegurar o respeito por “todas as normas aplicáveis em matéria de protecção de dados pessoais”, sempre com salvaguarda da confidencialidade e segurança desses dados (n.º 5).

A Decisão da Comissão de 28 de Fevereiro de 2004⁽⁶⁸⁾ aprovou o plano de trabalho para 2004 perspectivando a execução do programa de acção comunitária em matéria de saúde pública (2003-2008). Algumas das acções comunitárias pressupõem o tratamento sistematizado e informatizado de informação de saúde (cf. ponto 2.1.) e o «desenvolvimento de um «sistema sustentável de informação e conhecimento ao nível da UE». Estas acções passam por uma estratégia de desenvolvimento de atitudes concertadas de «análise de dados», «preenchimento das bases de dados e melhoria da qualidade e compatibilidade dos dados». Estes objectivos só se conseguem com a informatização da informação de saúde em aplicações compatíveis e com recolha de dados junto das entidades que, no terreno, fazem diagnóstico médico ou prestam cuidados de saúde.

⁽⁶⁷⁾ In Jornal Oficial L 271/1, de 9 de Outubro de 2002.

⁽⁶⁸⁾ Jornal Oficial L 60/58, de 27/2/2004.

Ao mesmo tempo, o ponto 2.1.6. desta Decisão salienta a necessidade de os Estados-Membros cooperarem entre si no desenvolvimento integrado de sistemas de informação de saúde capazes de responder aos desafios suscitados pela mobilidade dos pacientes e prestação de cuidados de saúde ao nível da União Europeia. Esta preocupação foi desenvolvida numa Comunicação da Comissão – *Com(2004) 301 final* – relativamente ao «acompanhamento do processo de reflexão de alto nível sobre a mobilidade dos doentes e a evolução dos cuidados de saúde na União Europeia». Nesta Comunicação foi dada particular atenção à «estratégia de informação dos sistemas de saúde» (ponto 3.1.), tendo sido evidenciadas as seguintes preocupações:

- A informação de saúde depende da capacidade dos cidadãos para usarem os sistemas de saúde, dos profissionais para diagnosticar, tratar ou dar seguimento e das autoridades sanitárias para planear e gerir os sistemas na sua globalidade;
- É fundamental dispor de informação relacionada com as prestações detalhadas de cuidados de saúde e estabelecimento de um enquadramento para a recolha sistemática de dados relativos ao volume e natureza dos movimentos de doentes.
- O programa relativo à informação sobre sistemas de saúde englobará o tratamento de “dados hospitalares, cuidados primários...esforços de prevenção e promoção da saúde”

Porém, foi a Comunicação (2004) 356 final, de 30 de Abril de 2004, da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões que veio definir a estratégia da «saúde em linha» como forma de “melhorar os cuidados de saúde para os cidadãos europeus”. Aí se preconiza que, até ao fim de 2005, cada Estado Membro deve proceder à “fixação de objectivos em matéria de interoperacionalidade e utilização dos dossiers clínicos electrónicos”.

O que está em causa, desde logo, é a necessidade de “identificar uma pessoa de maneira não ambígua”, reconhecendo-se que o plano de acção eEurope2005 “contém já o desenvolvimento

de normas para uma aproximação comum de identificação dos doentes e a arquitectura do dossier clínico electrónico”(69).

Até ao fim de 2006 os Estados-Membros, em colaboração com a Comissão Europeia, deveriam “determinar e definir as normas de interoperacionalidade para as mensagens relativas a dados de saúde e dossiers clínicos electrónicos, tendo em conta as boas práticas e os trabalhos de normalização nesta matéria”. Também se preconiza nesta comunicação, até ao fim de 2008, que os prestadores de cuidados de saúde estejam em condições de “fornecer serviços em linha tais como a teleconsulta, a prescrição electrónica, a orientação do paciente para um serviço especializado por via electrónica, e televigilância e a teleassistência”.

Os instrumentos acabados de citar ilustram as preocupações a nível comunitário e mostram qual o caminho que vai ser percorrido por parte de outros Estados-Membros.

2. Em França foi discutida, no decurso do corrente ano, a criação de um «*dossier* clínico informatizado» ou «*dossier* clínico partilhado» como forma de estabelecer mecanismos de acompanhamento do percurso dos doentes, promover a coordenação e continuidade dos cuidados de saúde. A criação deste suporte vai muito mais longe do que aquilo que preconizamos neste relatório.

O objectivo é o de centralizar, num único «*dossier* clínico», a informação relevante de cada paciente. Competirá a cada profissional de saúde integrar nesse *dossier*, no momento de cada acto médico ou consulta, «os elementos de diagnóstico e terapêutica relativos a cada pessoa por si prestados ou em cada estabelecimento de saúde»(70), reportando nesse suporte, de forma resumida, cada episódio em relação ao paciente.

(69) Respondendo a esta preocupação está em curso uma nova regulamentação do cartão de utente do Serviço Nacional de Saúde, tendo dado entrada nesta CNPD – para emissão do respectivo parecer – um projecto de Decreto-Lei que estabelece o regime jurídico do Sistema do Cartão de Utente do Serviço Nacional de Saúde.

(70) Veja-se a Deliberação da CNIL n.º 04-054 de 10 de Junho de 2004 in <http://www.cnil.fr>

Conforme se reconhece em relatório da Assembleia Nacional Francesa⁽⁷¹⁾, o «*dossier* clínico informatizado» *já existe de uma forma fraccionada*. Efectivamente, “os profissionais de saúde, e em particular cada médico, detêm informações diferentes sobre os pacientes, em locais diferentes (hospital, clínica, no consultório...)”. O recurso à automatização dos dados clínicos resulta da iniciativa e necessidade sentida da parte das instituições que prestam cuidados.

O objectivo agora prosseguido é o de “reunir alguns destes dados dispersos, armazená-los e colocar algumas informações facilmente acessíveis ao paciente e aos profissionais de saúde por ele autorizados, aproveitando as potencialidades das novas tecnologias de informação e comunicação”. Deste modo, será possível os médicos acederem aos dados mais relevantes dos doentes, independentemente do lugar onde os cuidados são prestados, abrindo caminho à possibilidade de assistência clínica a doentes fora do seu país.

A *Lei n.º 2004-810, de 13 de Agosto de 2004*, veio estabelecer, no seu artigo 5.º, que “um Decreto do Conselho de Estado, precedido de parecer da Commission National de l’Informatique et des Libertés, determina as condições em que um «*dado de identificação*» pode ser utilizado para a abertura e conservação do *dossier* clínico pessoal, tal como definido no artigo L 161-36-1 do Código de Segurança Social, no interesses da pessoa a que diz respeito e para fins exclusivos de coordenação dos cuidados”.

A criação de um *dossier* deste tipo em Portugal deverá, tal como em França, ser objecto de regulamentação por Lei da Assembleia da República.

3. Neste momento – e sem que haja necessidade de adoptar providências legislativas específicas (muito embora admitamos que se justifica uma melhor regulamentação no domínio do tratamento de alguns dados e em matéria de acesso à informação) – advogamos a necessidade de se caminhar para o tratamento automatizado como forma de assegurar a confidencialidade da informação de saúde e ultrapassar alguns problemas que o presente

⁽⁷¹⁾ *Rapport fait au nom de la Commission Spécialisé chargée d’examiner le projet de Loi (n.º 1675) relatif à l’assurance maladie* em que foi relator o deputado M. JEAN-MICHEL DUBERNARD (*in* <http://assemblee-nationale.fr>)

relatório evidenciou. Em particular, estamos convictos de que o «*dossier* clínico informatizado» irá trazer vantagens acrescidas em diversos domínios, nomeadamente:

- a) Será assegurada, através da separação lógica entre dados administrativos e de saúde, a possibilidade de limitar o acesso de certos profissionais a dados dos doentes. O acesso à informação de saúde ficará, assim, limitado aos dados que o profissional necessita para fins de diagnóstico, tratamento e prestação de cuidados;
- b) É possível «segmentar» o acesso à informação constante da ficha clínica, limitando o acesso a determinados profissionais de saúde (v.g. o «médico assistente) a informação mais sensível (v.g. hábitos sexuais, parceiros) que o doente pretenda preservar do conhecimento de terceiros;
- c) A informação necessária à prestação de cuidados ficará rapidamente acessível aos profissionais que dela precisem para esse efeito, evitando situações de impossibilidade ou dificuldade de localização da ficha clínica, de meios auxiliares de diagnóstico (que nem sempre são integrados no processo clínico). Deste modo, será afastada a possibilidade de haver, dentro do mesmo estabelecimento, informação clínica dispersa e acessível, exclusivamente, a determinado serviço e que não é integrada no processo clínico do doente.
- d) Ao ser criado este «*dossier* clínico informatizado» serão adoptados, necessariamente, mecanismos que permitem o pedido em tempo real de meios auxiliares de diagnóstico, através da rede do hospital, bem como a partilha e consulta *on line* dos respectivos resultados por parte dos profissionais autorizados. Deste modo, poderão ser criados arquivos específicos no domínio da patologia clínica e da imagiologia.
- e) Poderão ser adoptados procedimentos técnicos que permitam, com grande facilidade, a obtenção de dados não nominativos destinados à investigação científica, à definição de estratégias de prevenção ou a fins de saúde pública, sempre com preservação da confidencialidade e privacidade dos doentes.
- f) Serão, gradualmente, abandonados os suportes de papel e afastados os riscos para a privacidade que advêm da acessibilidade do processo clínico a pessoas não autorizadas.

CONCLUSÕES

1. Em relação à omissão da obrigação de notificação verifica-se que, apesar de a generalidade dos hospitais estarem conscientes de que devem fazer as respectivas notificações, não houve da sua parte a preocupação de fazer um levantamento exaustivo dos tratamentos existentes. Não se aceita que a generalidade dos hospitais mantenha uma percentagem elevada de tratamentos não notificados (cerca de 50%).
2. Em nenhum Hospital – à excepção daqueles onde havia avisos afixados a informar sobre a recolha de imagens no âmbito da videovigilância – foram adoptados mecanismos concretos que se destinem a assegurar o *direito de informação dos titulares dos dados*.
3. O direito de informação não é assegurado nos moldes em que é exigido pelo artigo 10.º da Lei 67/98, de 26 de Outubro.
4. Quando o Hospital, na qualidade de responsável pelo tratamento, pretender facultar os dados dos doentes para fins de investigação científica deve certificar-se de que essa finalidade foi notificada e autorizada pela CNPD. Isso não tem acontecido porque os processos clínicos têm vindo a ser facultados sem qualquer controlo da CNPD. ***Neste particular há um generalizado incumprimento da lei.***
5. A menos que a CNPD entenda, em concreto, que um projecto de investigação científica se fundamenta em «*motivo de interesse público importante indispensável ao exercício das atribuições legais ou estatutárias do responsável*» – o que dificilmente se verifica dado o alcance restritivo que tem vindo a ser dado à previsão do artigo 7.º n.º 2 da Lei 67/98 – o *acesso aos dados nominativos dos doentes* no âmbito daquela finalidade só pode ser facultado se for assegurado o *consentimento dos doentes*.
6. A menos que haja disposição específica sobre prazos de conservação de dados de saúde, deverão os hospitais observar as disposições e prazos de conservação estabelecidos na Portaria n.º 247/2000, de 8 de Maio.

7. Os profissionais de saúde não podem instalar aplicações informáticas de gestão da prestação de cuidados de saúde à revelia do responsável do tratamento e sem o controlo CNPD.
8. Se isso acontecer só uma solução alternativa se admite:
 - a) Haver um acordo entre o profissional de saúde e o Hospital que garanta que a informação processada apenas pode ser tratada no interior do Serviço. Deve ser garantido que, em caso algum, nenhum médico do serviço pode «apropriar-se» da informação, para fins estritamente privados. A aplicação deve ser notificada à CNPD, sendo responsável o Hospital ou o Serviço onde se encontra instalada a aplicação.
 - b) Se não houver acordo e o profissional de saúde continuar a reclamar a «titularidade privada» da aplicação entende-se que o tratamento em causa deve cessar, ainda que devam ser adoptadas metodologias de recuperação da informação para assegurar a continuidade de prestação de cuidados de saúde aos utentes do serviço.
9. O acesso indiscriminado aos sistemas de videovigilância, nomeadamente se captarem a entrada de pessoas em determinados serviços, pode consubstanciar um desvio da finalidade (porque passível de documentar informação de saúde das pessoas filmadas) e envolver a violação da sua privacidade ou, mesmo, contribuir para a sua discriminação.
10. A instalação destes sistemas – especialmente vocacionados para detectar a entrada de pessoas estranhas ao serviço – devem sempre preservar a intimidade dos doentes. As imagens gravadas não devem ser visionadas, limitando-se os responsáveis a entregá-las às autoridades policiais sempre que haja suspeita ou participação da prática de crimes.
11. O recurso à *telemedicina* deve ser institucionalizado e não deve ficar exclusivamente dependente do impulso e iniciativa de profissionais de saúde ao ponto de poder diminuir ou cessar a sua utilização se determinado profissional mais entusiasta abandona o hospital. O direito de informação dos utentes deve ser garantido.

12. No momento em que as redes hospitalares cobrem, na generalidade dos casos, todos os serviços dos hospitais e não são excessivamente dispendiosas ferramentas (nalguns casos já disponíveis) que viabilizam os pedidos de análises clínicas em tempo real através da rede, importa que os hospitais dêem prioridade à adopção das medidas técnicas necessárias que assegurem a requisição *on line* destes pedidos.
13. Esta medida contribuirá, de forma decisiva, para reforçar a confidencialidade em relação à informação clínica e para garantir que o acesso àquela informação é reservado aos profissionais de saúde que dela necessitem para o exercício das suas funções.
14. Pela mesma ordem de fundamentos justifica-se que os resultados das análises possam ser consultados *on line* pelos serviços requisitantes e que estejam acessíveis, em tempo real, a alguns serviços para obviar à requisição de exames desnecessários.
15. O facto de o processo clínico se encontrar em suporte de papel é motivo bastante para considerar que, por mais esforços que sejam feitos, existem sempre riscos de a informação clínica ser acessível por terceiros não autorizados.
16. O processo clínico em papel encontra-se, por natureza, exposto à curiosidade geral – quer no próprio arquivo, quer nos serviços por onde circula – não havendo mecanismos eficazes que assegurem a impossibilidade de devassa.
17. A CNPD considera que só os suportes automatizados dotados das necessárias seguranças – *passwords* com «perfis de utilizadores» bem definidos, separação lógica entre dados administrativos e de saúde – podem conferir a necessária confidencialidade à informação clínica dos doentes.
18. O «*dossier* clínico informatizado» irá trazer vantagens acrescidas em diversos domínios, nomeadamente:
 - a) Será assegurada, através da separação lógica entre dados administrativos e de saúde, a possibilidade de limitar o acesso de certos profissionais a dados dos doentes.

- b) O acesso à informação de saúde ficará, assim, limitado aos dados que o profissional necessita para fins de diagnóstico, tratamento e prestação de cuidados;
- c) É possível «segmentar» o acesso à informação constante da ficha clínica, limitando o acesso a determinados profissionais de saúde (v.g. o «médico assistente) a informação mais sensível (v.g. hábitos sexuais, parceiros) que o doente pretenda preservar do conhecimento de terceiros;
- d) A informação necessária à prestação de cuidados ficará rapidamente acessível aos profissionais que dela precisem para esse efeito, evitando situações de impossibilidade ou dificuldade de localização da ficha clínica, de meios auxiliares de diagnóstico (que nem sempre são integrados no processo clínico).
- e) Deste modo, será afastada a possibilidade de haver, dentro do mesmo estabelecimento, informação clínica dispersa e acessível, exclusivamente, a determinado serviço e que não é integrada no processo clínico do doente.
- f) Ao ser criado este «*dossier* clínico informatizado» serão adoptados, necessariamente, mecanismos que permitem o pedido em tempo real de meios auxiliares de diagnóstico, através da rede do hospital, bem como a partilha e consulta *on line* dos respectivos resultados por parte dos profissionais autorizados.
- g) Deste modo, poderão ser criados arquivos específicos no domínio da patologia clínica e da imagiologia.
- h) Poderão ser adoptados procedimentos técnicos que permitam, com grande facilidade, a obtenção de dados não nominativos destinados à investigação científica, à definição de estratégias de prevenção ou a fins de saúde pública, sempre com preservação da confidencialidade e privacidade dos doentes.
- i) Serão, gradualmente, abandonados os suportes de papel e afastados os riscos para a privacidade que advêm da acessibilidade do processo clínico a pessoas não autorizadas.

RECOMENDAÇÕES

1. A CNPD recomenda que os hospitais façam um levantamento exaustivo de todas as aplicações de gestão de informação de saúde, fazendo em seguida a respectiva notificação à Comissão.
2. Todos os *formulários* existentes nos hospitais e que se destinem a recolher dados pessoais junto dos utentes devem ser reformulados por forma a assegurarem o *direito de informação* – nos termos consignados no artigo 10.º n.º 1 e 2 da Lei 67/98 – devendo, ao mesmo tempo, ser obtido o consentimento para o tratamento de dados quando esse consentimento se revelar necessário (cf. artigo 7.º n.º 2 da Lei 67/98) e o titular dos dados estiver em condições de poder prestar esse consentimento (veja-se o disposto no artigo 7.º n.º 3 alínea a) da Lei 67/98).
3. A informação sobre a existência de tratamento poderá ser verbal sempre que os dados sejam recolhidos por inquérito verbal junto dos titulares, sendo desejável que, nos locais onde tais dados são sistematicamente recolhidos, haja avisos afixados que forneçam tais informações.
4. Apresentando-se as limitações ao *direito de acesso* como excepcionais, será de admitir que a regra geral contida no artigo 11.º n.º 5 da Lei 67/98 pode ter de sofrer uma inflecção.
5. Daí que se recomende a necessidade de ponderar, em termos legislativos, se deve continuar a manter-se a regra do «acesso por intermediação» de médico. Caberá à Assembleia da República ponderar e legislar sobre esta matéria.
6. Quando os dados pessoais dos utentes forem utilizados para *investigação científica* deverão ser adoptados mecanismos de informação e de consentimento informado.

7. Dada a inexistência de disposições legais que regulem o acesso à informação clínica para fins de investigação científica – *legislação que deveria ser preparada para viabilizar ou facilitar projectos de investigação de relevante interesse científico* – a utilização nominativa dessa informação só pode ocorrer por via do *consentimento* (cf. o artigo 35.º n.º 3 da Constituição da República e art. 7.º n.º 2 da Lei 67/98).
8. A forma como estão a ser utilizados os dados dos doentes para investigação científica deve ser objecto de uma ampla reflexão por parte das Administrações dos Hospitais, devendo ser alterados os procedimentos actualmente existentes para os conformar com os preceitos legais hoje vigentes.
9. Também o Governo e Assembleia da República devem reflectir sobre esta problemática, a fim de poderem tomar as medidas legislativas adequadas.
10. Os hospitais devem investir mais na formação e sensibilização dos utilizadores por forma a evitar que ocorram «falhas» ao nível da segurança dos sistemas.
11. Por outro lado, é desejável que sejam adoptados procedimentos escritos claros que definam regras de acesso à informação, critérios a adoptar na atribuição de *passwords*, obrigatoriedade de alteração de *passwords* com determinada periodicidade, bem como a adopção de procedimentos técnicos que obriguem os utilizadores a digitar de novo o seu *login* e *password* sempre que a aplicação, uma vez «aberta», não tenha sido utilizada durante um determinado período de tempo.
12. É fundamental que os Hospitais notifiquem os tratamentos de videovigilância, especificando com rigor quais as finalidades prosseguidas e as condições concretas em que são captadas as imagens para permitir à CNPD – no âmbito das suas competências de *controlo prévio* (cf. artigo 28.º n.º 1 al. a) da Lei 67/98) – fixar algumas das condições necessárias a preservar a confidencialidade dos titulares dos dados.

13. As novas tecnologias utilizadas no âmbito da telemedicina suscitam novos problemas jurídicos que devem ser equacionados quer no quadro tradicional das relações entre os médicos e os doentes, quer ao nível da responsabilidade médica.
14. Por uma questão de certeza e segurança em relação à especificidade da tecnologia utilizada, não deverá ser negligenciada a possibilidade de haver uma entidade certificadora da qualidade destes sistemas.
15. No que diz respeito ao enquadramento legal da telemedicina seria desejável que a Assembleia da República ponderasse a necessidade de estabelecer alguns princípios jurídicos reguladores. A utilização desta tecnologia, que se diz poder vir a ser generalizada com o objectivo de ultrapassar algumas dificuldades como a falta de médicos de determinadas especialidades em certos hospitais, deveria ser acompanhada de disposições legais que vinculassem os responsáveis a cumprir alguns dos procedimentos enunciados.
16. Dispondo os hospitais de redes que cobrem, em geral, todos os serviços, recomenda a CNPD que se privilegie a circulação da informação clínica através da rede, em detrimento da utilização de suportes de papel.
17. Este procedimento deve ser utilizado, nomeadamente, em relação ao pedido e consulta de meios auxiliares de diagnóstico (v.g. imagiologia e análises clínicas).
18. Sabendo-se que o SAM dispõe de ferramenta que permite assegurar o cumprimento destes objectivos, lança a CNPD um desafio ao IGIF para, na medida do possível, colocar este objectivo na sua agenda de prioridades. Esta alteração melhorará, de forma significativa, a confidencialidade da informação no interior dos hospitais.
19. A CNPD considera que, à semelhança do que acontece com outras realidades da actividade económica (registos e notariado, contribuições impostos, informação contabilística), é necessário que se tomem medidas legislativas clarificadoras

que confirmam força probatória similar aos suportes automatizados utilizados em ambiente hospitalar.

20. Esta solução dissiparia quaisquer dúvidas que têm vindo a ser colocadas e que são um obstáculo relevante à institucionalização de medidas – que muitos hospitais pretendem e advogam – que visam a automatização do processo clínico e a digitalização dos suportes de papel hoje existentes.
21. O estudo de soluções que apontam para a criação de um *dossier* clínico informatizado e para a digitalização do processo clínico em suporte de papel *deve ser, na nossa óptica, uma prioridade a considerar pelo Ministério da Saúde.*
22. Neste momento – e sem que haja necessidade de adoptar providências legislativas específicas (muito embora admitamos que se justifica uma melhor regulamentação no domínio do tratamento de alguns dados e em matéria de acesso à informação) – defendemos a necessidade de se caminhar para o tratamento automatizado como forma de assegurar a confidencialidade da informação de saúde e ultrapassar alguns problemas que o presente relatório evidenciou.
23. À semelhança do que acontece noutros países (v.g. França e Bélgica), considera a CNPD que a Assembleia da República deveria legislar sobre as condições em que os hospitais ou os médicos poderiam facultar o acesso a dados de saúde a terceiros (em particular Companhias de Seguros) após a morte dos titulares dos dados.

ANEXOS

A

LISTA DOS HOSPITAIS VISITADOS (38 HOSPITAIS)

1. HOSPITAL DE SANTA CRUZ, S.A. - LISBOA
2. HOSPITAL SÃO FRANCISCO XAVIER - LISBOA
3. HOSPITAL DE EGAS MONIZ, S.A. - LISBOA
4. CENTRO HOSPITALAR DE LISBOA – ZONA CENTRAL (S.JOSÉ)
5. HOSPITAL DE SANTA MARTA, S.A. - LISBOA
6. HOSPITAL SGHD – SOCIEDADE GESTORA DO HOSPITAL DAS DESCOBERTAS, S.A.
7. HOSPITAL DOS SAMS – SERVIÇOS DE ASSISTÊNCIA MÉDICO-LEGAL DO S.B.S.I. - LISBOA
8. HOSPITAL AMADORA/SINTRA – SOCIEDADE GESTORA, S.A.
9. HOSPITAL GARCIA DE ORTA, S.A - ALMADA
10. HOSPITAL DE NOSSA SENHORA DO ROSÁRIO, S.A. - BARREIRO
11. HOSPITAL DE S. BERNARDO, S.A. - SETÚBAL
12. HOSPITAL DO LITORAL ALENTEJANO - SANTIAGO DO CACÉM
13. CENTRO HOSPITALAR DE CASCAIS / HOSPITAL CONDE CASTRO GUIMARÃES - CASCAIS
14. HOSPITAL NOSSA SENHORA DA OLIVEIRA – GUIMARÃES *
15. HOSPITAL DE S. SEBASTIÃO – SANTA MARIA DA FEIRA
16. HOSPITAL DE SÃO MARCOS – BRAGA
17. HOSPITAL DE SANTO ANTÓNIO – PORTO
18. HOSPITAL MAGALHÃES DE LEMOS – PORTO
19. CENTRO HOSPITALAR DO BARLAVENTO ALGARVIO, S.A. - PORTIMÃO
20. CENTRO HOSPITALAR DA COVA DA BEIRA, SA – COVILHÃ
21. CENTRO HOSPITALAR DE COIMBRA
22. HOSPITAL DA UNIVERSIDADE DE COIMBRA
23. HOSPITAL INFANTE D. PEDRO, S.A. – AVEIRO
24. HOSPITAL DISTRITAL DA FIGUEIRA DA FOZ, S.A.
25. CENTRO HOSPITALAR DO BARLAVENTO ALGARVIO, S.A. - LAGOS
26. HOSPITAL DO ESPÍRITO SANTO – ÉVORA
27. CENTRO HOSPITALAR DO MÉDICO TEJO, S.A. – HOSP. DR. MANUEL CONSTÂNCIO - ABRANTES
28. HOSPITAL DISTRITAL DE SANTARÉM, S.A.
29. HOSPITAL DE SANTA LUZIA – ELVAS
30. HOSPITAL JOSÉ JOAQUIM FERNANDES, SA – BEJA
31. HOSPITAL DE SÃO PAULO, S.A. – SERPA

32. HOSPITAL AMATO LUSITANO – CASTELO BRANCO
33. HOSPITAL DE SÃO TEOTÓNIO, S.A. – VISEU
34. HOSPITAL CENTRAL DO FUNCHAL
35. CENTRO DE SAÚDE DE VILA FRANCA DO CAMPO
36. CENTRO DE SAÚDE DA RIBEIRA GRANDE
37. HOSPITAL DIVINO ESPIRITO SANTO – PONTA DELGADA
38. CENTRO HOSPITALAR DE VILA REAL / PESO DA RÉGUA

B
GERAL

Entidade.....

Inquirido – Nome **Tel.**

1. Aplicações notificadas à CNPD Não Sim

.....**Conforme c/ notific/** Não Sim

.....**Conforme c/ notific/** Não Sim

.....**Conforme c/ notific/** Não Sim

.....**Conforme c/ notific/** Não Sim

.....**Conforme c/ notific/** Não Sim

.....**Conforme c/ notific/** Não Sim

.....**Conforme c/ notific/** Não Sim

2. Arquivo único Centralizado Não Sim

3. Rede que cobre todo o Hospital/CSaúde Não Sim

4. Regras sobre acesso à informação Não Sim

Escritas **Caso a caso** **Conforme o Serviço** **Outras**

Quais

5. Há experiências de Telemedicina? Não Sim **Quais?**

1..... **Hospitais**

2..... **Hospitais**

Videovigilância Não Sim **Notificado** Não Sim

Observações finais

.....

.....

C

BASES DE DADOS

Entidade.....Serviço

Inquirido – Nome Tel.

1. Existe aplicação informática p/ gestão de doentes? Não Sim

Nome da aplicação Em rede Computador isolado

Trata **apenas** os dados administrativos p/ localização da ficha clínica

Trata dados administrativos e informação clínica

A informação clínica está suportada em **tabelas**? Sim Não

Quais? ICD Outras **Texto livre** Sim Não

Password? Sim Não Backups Sim Não Periodicidade

Está notificada à CNPD Sim Não

2. **Finalidade**: Cuidados de saúde Facturação Inv. Científica

3. **Dados sensíveis**: Raça Religião Toxicoddependência/Droga

HIV Sexuais Parceiros Prostituição Genéticos Problemas Sociais e de
integração Outros.....

Acessíveis a quem?.....

4. **Quem introduz os dados de saúde na aplicação?**

O médico O funcionário administrativo O enfermeiro/técnico de saúde Outro
.....

5. É assegurado **direito de informação** aos doentes? Não Sim

Como? P/ escrito Verbal Afixação no local da recolha

6. **Separação lógica**: dados administrativos/saúde? Sim Não

Níveis de acesso à informação Não Sim

1..... 2.....

3.....4.....

7. Que m pode consultar a ficha clínica (resposta múltipla)?

Qualquer médico do Hospital *Qualquer médico do serviço*

Apenas o médico que tem consulta marcada *Qualquer funcionário administrativo* *Qualquer funcionário do Hospital* *O médico do hospital para investigação científica* *Qualquer médico para investigação científica*

Outras pessoas

8. Como se exerce o direito de acesso? Dirigido a quem?.....

.....*Directo pelo doente* *Por intermediação de médico*

9. Regras p/ acesso à f. clínica – investigação científica? Não Sim

Qualquer pessoa desde que inserido em projecto de investigação *Qualquer médico* *Apenas com o consentimento do doente* *Desde que os dados sejam anonimizados* *Desde que o projecto seja relevante* *Outras condições*

10. A ficha clínica pode sair do Hospital? Não Sim

Condições.....

11. Há regras sobre prazos de conservação de dados? Não Sim

Quando são eliminados? Permanentes *Outro prazo*

Observações finais.....

.....

.....

D

Arquivo Clínico

Entidade

Inquirido – Nome **Tel.**

1. Arquivo Centralizado – Sim **Não** **Outro**

2. Ficha Clínica única para cada doente – Sim **Não**

3. Existe aplicação informática para gestão da ficha clínica? Não Sim

Apenas os dados administrativos para localização da ficha clínica

Dados administrativos e informação clínica

Tem *password*? Sim Não

Backups Não Sim Periodicidade

Está notificado à CNPD Sim Não

4. Regulamento para acesso/consulta da ficha clínica – Não Sim (**cópia**)

5. Há registo da entrada/saída/requisição de processos clínicos – Não Sim

Manual Informático

Notificado à CNPD Sim Não

6. Quem pode pedir as fichas clínicas (resposta múltipla)?

Qualquer médico do Hospital *Apenas o médico que tem consulta marcada*

Qualquer funcionário administrativo *Qualquer profissional de Saúde*

Qualquer funcionário do Hospital *O médico para investigação científica*

Outras pessoas

.....

7. Quem transporta a ficha clínica para a consulta?

A pessoa indicada pelo serviço a que se destina a ficha *Qualquer pessoa* *Funcionário do*

arquivo *Funcionário administrativo*

Outros. Quais?.....

.....

8. Como circula a ficha clínica no interior do Hospital?

Caixa ou recipiente fechado *Em pasta* (que pode ser aberta) *Em «lotes» de acordo com as consultas* *Outra*

9. Quem aprecia o pedido de acesso à f. clínica (v.g. seguradoras e terceiros)?

Direcção do Hospital *Director Clínico* *Responsável do arquivo*

Os serviços jurídicos *Outros*

10. Há regras de acesso à ficha clínica para fins de investigação científica? Não Sim

Qualquer pessoa pode solicitar desde que inserido em projecto de investigação

Qualquer médico a pode solicitar *Apenas com o consentimento do doente*

Se não há consentimento apenas se os dados forem anonimizados

Desde que o projecto seja relevante/sem consentimento

Outras condições

11. A ficha clínica pode sair do Hospital? Não Sim

Condições

Observações finais

.....

.....

E

ANÁLISES CLÍNICAS

Entidade.....Serviço

Inquirido – Nome Tel.

1. Há aplicação informática p/ gestão de análises? Não Sim

Nome da aplicação Em rede Computador isolado

Trata apenas dados administrativos Não Sim

É registado o diagnóstico «possível» quando indicado? Não Sim

Password? Sim Não Backups Sim Não Periodicidade

Está notificada à CNPD Sim Não

2. Dados sensíveis: Raça Religião Toxicod dependência/Droga

HIV Sexuais Parceiros Prostituição Genéticos Problemas Sociais e de
integração Outros.....

Acessíveis a quem?

3. Os pedidos da análises: Em papel Pela rede do Hospital

Quando em papel: Sempre em carta fechada Nunca Só quando vem anotado o diagnóstico
possível Variável em função do serviço

4. O funcionário administrativo (que marca as análises) tem acesso ao «diagnóstico possível» Não

Marca com base no nome

Há medidas adoptadas que o impedem de ter acesso ao diagnóstico

Sim O pedido do médico é-lhe entregue Não há outros cuidados

5. É assegurado direito de informação aos doentes? Não Sim

Como? *P/ escrito* *Verbal* *Afixação no local da recolha*

6. O acesso aos resultados é feito: Em papel

Por entrega ao doente *Enviados ao médico/serviço requisitante*

Informaticamente

O médico pode consultá-los pela rede do hospital

Os resultados são enviados pela rede ao serviço requisitante

Outro.....

7. Há regras sobre prazos de conservação de dados? Não Sim

Quando são eliminados? *Permanentes* *Outro prazo*

Observações finais.....

.....

.....