COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

AUTORIZAÇÃO N.º 5114 /2012

I. Do Pedido

A Clínica CUF Belém, S.A. notificou à CNPD um tratamento de dados pessoais com a finalidade de disponibilização aos utentes, através da Internet, de resultados/relatórios de meios complementares de diagnóstico, do histórico de consultas e exames realizados e possibilidade de marcação de consultas (Serviço MyCUF).

A responsável pelo tratamento presta serviços na área da saúde, designadamente consultas, realização de exames médicos e tratamentos médicos.

A. Da Informação Constante do MyCUF

Com vista a possibilitar ao utente uma visão integrada sobre a sua atividade junto das Unidades de Saúde CUF, o responsável pelo tratamento disponibiliza um sítio na Internet por unidade de saúde.

Com efeito, em cada um deles é possível o acesso do utente aos seus resultados de exames, independentemente da Unidade de Saúde CUF onde foram realizados.

Do mesmo modo, é também permitido ao utente consultar o seu histórico de episódios clínicos e efetuar a marcação de consultas.

Com esse propósito, são tratados os seguintes dados:

- Registo no MyCUF: nome, telefone, correio eletrónico, data de nascimento, nome de utilizador e palavra-chave;

- Marcação de consultas/Exames: unidade em que pretende a consulta/exame, especialidade, ato médico, médico para que pretende marcar o episódio médico, data e hora da marcação, entidade financeira responsável pelo pagamento, observações indicadas pelo utilizador, digitalização submetida pelo utilizador, n.º de cliente (para

clientes autenticados), nome, data de nascimento, telefone e correio eletrónico (para clientes não autenticados);

- Histórico de episódios: especialidade, ato e rúbrica do episódio realizado, unidade de saúde em que se realizou, data de início e fim do episódio, estado do episódio, profissional de saúde que executou o episódio, n.º de episódio, tipo de episódio, indicação se existem resultados do episódio e identificador desses resultados e n.º de cliente que realizou o episódio.

B. Da Arquitetura do MyCUF

Os sistemas responsáveis pela gestão da informação dos utentes dentro das várias unidades de saúde CUF (identificados como "sistemas operacionais") formam os principais repositórios de informação sobre os quais assenta o sistema MyCUF. Assim, a informação encontra-se dispersa pelas várias unidades de saúde, não sendo este sistema suportado por um único repositório de dados centralizado. Cada unidade alberga os seus próprios sistemas operacionais, nas suas instalações.

De forma a permitir o acesso dos utentes às suas informações, o grupo JMS implementou um sistema que interliga os sistemas operacionais com um servidor web, possibilitando a disponibilização de conteúdos na Internet.

O servidor web é responsável pela apresentação dos conteúdos ao utente numa página web. Este servidor comunica diretamente com os servidores aplicacionais que são os responsáveis por toda a lógica envolvida no sistema MyCUF. Estes últimos organizam e direcionam todos os pedidos que resultam da atividade do utilizador na página web para os repositórios locais de informação.

Os servidores aplicacionais estão implementados recorrendo à tecnologia OutSystems sobre tecnologia Microsoft.

Existe um servidor de bases de dados com uma função de apoio aos servidores aplicacionais que armazena a informação necessária para que os pedidos web possam ser atendidos em tempo útil.

Os utentes acedem aos sítios web das múltiplas unidades de Saúde CUF através da Internet, utilizando dispositivos que possam trocar informação através de protocolo HTTP ou HTTPS. A informação comercial e institucional pública será transacionada usando o protocolo HTTP, enquanto a informação pessoal será sempre transacionada usando o protocolo HTTPS.

Indica a responsável pelo tratamento que *"todos os pedidos provenientes da Internet atravessam uma firewall, protegendo os servidores aplicacionais de ataques em portos diferentes dos esperados. Esta firewall garante o isolamento do servidor de base de dados para que o mesmo não seja acedido por outras máquinas, que não os servidores aplicacionais"*.

Os servidores web, aplicacionais e de base de dados encontram-se em território nacional e alojados nas instalações da ONI, sem qualquer referência ao nome da pessoa a que respeita, sendo apenas identificável através de um número de cliente que não é público e que, sem os restantes serviços e sem consulta aos sistemas operacionais do Grupo José Mello Saúde, não permite ligar a informação armazenada a uma pessoa concreta.

Todas as máquinas que suportam o MyCUF são propriedade da José Mello Saúde e de uso exclusivo para este sistema.

Os servidores aplicacionais são responsáveis por preparar toda a informação disponibilizada aos utilizadores, podendo – para efeitos de desempenho – ter em sessão dados pessoais dos utilizadores. Estes dados são apenas acessíveis ao utilizador para quem está criada a sessão HTTPS e apenas existem durante o decurso da sessão, sendo eliminados com o final da mesma.

C. Da Autenticação no MyCUF

O processo de adesão ao MyCUF inicia-se quando o cliente manifesta pessoalmente o seu interesse em aderir aos serviços MyCUF, num balcão de uma Unidade CUF. Na sequência desse facto, o operador do balcão identifica o cliente através do cartão de cidadão, regista no sistema operacional a vontade do cliente em aderir ao MyCUF, o tipo e número de documento de identificação e o correio eletrónico do cliente.

O sistema operacional indica ao servidor aplicacional a vontade do cliente em aderir aos serviços MyCUF, referindo o número desse cliente, o seu nome e endereço de correio eletrónico. Em seguida, o sistema aplicacional envia um *e-mail* de convite ao cliente, que conterá uma ligação única que permite identificar o convite enviado. Seguindo essa ligação, é solicitado ao cliente que insira o n.º do documento de identificação indicado pessoalmente, bem como que crie o seu nome de utilizador e palavra-chave desejados. A palavra-chave deverá conter no mínimo seis carateres.

Por consulta ao sistema operacional, o sistema aplicacional confirma a validação dos dados, cria a conta daquele utilizador, permitindo o acesso aos serviços MyCUF.

O acesso *on-line* será permitido mediante prévia identificação e autenticação, e será restrito aos dados respeitantes à pessoa do utilizador, armazenados nos sistemas operacionais das unidades de saúde privadas do Grupo José Mello Saúde, nomeadamente Hospital CUF Infante Santo, Hospital CUF Descobertas, Hospital CUF Porto, Clínica CUF Alvalade, Clínica CUF Cascais, Clínica CUF Torres Vedras, Clínica CUF Belém e Instituto CUF de Diagnóstico e Tratamento.

O utilizador autenticado poderá aceder à informação de saúde de menores de dezasseis anos, desde que previamente tenha feito prova da representação legal sobre o menor ou da titularidade do respetivo poder parental. Quando o menor atingir dezasseis anos, o utilizador pai/representante deixará de ter acesso aos seus dados.

Nenhum utilizador acederá à informação de outros utilizadores, salvo a exceção *supra* descrita.

D. Do Acesso ao MyCUF

O serviço MyCUF regista os seguintes *logs* de acesso: nome de utilizador, data e hora, IP de origem, registo de sucesso ou insucesso na tentativa de entrada em sessão e *hash* criptográfico e qual a informação a que acede.

Não é permitido a um utilizador que, na mesma sessão, falhe três vezes consecutivas o acesso se autentique nos seguintes cinco minutos, tal como não é permitida qualquer tentativa de autenticação proveniente de um IP que tenha produzido dez tentativas consecutivas de autenticação falhadas.

E. Da Subcontratação dos Serviços

As entidades subcontratadas neste tratamento de dados pessoais são: HP para apoio técnico de *hardware*, a ONI Telecom - Infocomunicações, S.A. disponibiliza as instalações para armazenamento das máquinas da JMS, garantindo as condições técnicas de suporte físico, e a empresa Truewind-Chiron tem a seu cargo a gestão/manutenção de software, incluindo serviços de monitorização, Administração e Service Desk dos servidores.
Ao nível do sistema operativo a Truewind-Chiron e o Grupo José Mello Saúde têm direitos exclusivos de administração sobre todos os servidores.

No contrato ou ato jurídico, o qual revestirá a forma escrita, com valor probatório legalmente reconhecido, deve constar que o subcontratante apenas atua mediante instruções do responsável pelo tratamento e que lhe incumbe a obrigação de pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, bem como para garantir um nível de segurança

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

adequado em relação aos riscos inerentes ao tratamento e à natureza dos dados a proteger (cfr. artigo 14.º da LPD).

II. Da Análise

Foi solicitado um parecer ao Conselho de Ética da José de Mello Saúde, que se pronunciou no seguinte sentido:

1. *Uma vez observados os princípios da privacidade e confidencialidade dos dados (que aqui não estão em causa nem em discussão), é eticamente aceitável que a informação de saúde contida nos exames de diagnóstico seja disponibilizada por qualquer suporte, de papel ou informático ao seu titular (o utente) sem necessidade de intermediação médica.*
2. *Sendo que o recurso a meios informáticos pretende, com maior eficácia, reproduzir o procedimento físico tradicional, constitui uma discriminação para o utente ver diminuída ou colocada em risco a eficácia do procedimento informático que visa exclusivamente facilitar a sua vida pessoal em substituição do mesmo procedimento praticado há anos em suporte papel.*
3. *Não há qualquer razão plausível que explique por que há-de ser tutelada a autonomia dos doentes de hospitais públicos e coartada a dos que se dirigem a estabelecimentos privados. O regime que só impõe intermediação médica se o utente a requerer deve ser observado por todos os estabelecimentos que disponibilizam dados de saúde e, por conseguinte, também pelas unidades de saúde CUF.*

Por outro lado, o n.º 4 do artigo 7.º da Lei n.º 67/98, de 26 de outubro admite o tratamento de dados de saúde quando for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou para gestão dos serviços de saúde, desde que o tratamento desses dados seja efectuado por profissional de saúde sujeito a sigilo médico ou por outra pessoa obrigada a segredo profissional e desde que estejam garantidas medidas de segurança da informação.

O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados, as quais devem assegurar um nível de protecção adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger (cfr. n.º1 do artigo 14.º da LPD).

Estando em causa o tratamento de dados pessoais sensíveis, como é o caso, o responsável pelo tratamento de dados deve adoptar as medidas de segurança da informação previstas no artigo 15.º da LPD. Tais medidas devem aplicar-se tanto aos dados contidos em ficheiros automatizados, como aos dados manuais. Importa ainda ter em atenção os procedimentos concretos quanto às formas de recolha, processamento e circulação da informação.

A CNPD determina, ao abrigo do n.º 4 do artigo 15.º da LPD, que a circulação da informação em rede, porque pode pôr em risco direitos, liberdades e garantias dos titulares, deve ser encriptada. O sistema deve garantir uma separação lógica entre os dados referentes à saúde e os restantes dados pessoais, de natureza administrativa (cfr. n.º 3 do artigo 15.º da LPD).

Independentemente das medidas de segurança adotadas pela entidade responsável pelo tratamento, é a esta que cabe assegurar o resultado da efetiva segurança da informação e dos dados tratados.

Alerta-se que, deve ser criado um período de *time out*, sendo bloqueada a sessão para o utilizador que ultrapasse um período de inatividade na sessão de cinco minutos.

Devem, pois, ser adoptadas medidas de segurança que impeçam o acesso à informação a pessoas não autorizadas.

Ainda no âmbito das condições de segurança, devem ser feitas cópias de segurança (backups) da informação, as quais deverão ser mantidas em local apenas acessível ao administrador de sistema ou, sob sua direcção, a outros técnicos obrigados a segredo profissional. No que diz respeito aos dados contidos em suporte de papel, devem ser

adoptadas medidas organizacionais, que garantam um nível de segurança idêntico, impedindo acesso e manuseamento indevidos.

O fundamento de legitimidade é o consentimento dos titulares dos dados. Relativamente aos dados dos menores, os seus representantes legais – desde que previamente tenham feito prova da paternidade ou da titularidade do poder paternal – terão acesso à informação até que os mesmos completem dezasseis anos.

No que respeita às tentativas de autenticação, a CNPD entende que após três tentativas falhadas, deve ser bloqueado o acesso, sendo necessário pedir nova senha de autenticação.

Adverte esta Comissão para a necessidade do responsável pelo tratamento proceder, no âmbito de auditoria interna, a análises periódicas dos *logs* de acesso, com vista à deteção de eventuais acessos indevidos, devendo elaborar relatórios dessas auditorias e mantê-los à disposição da CNPD, pelo período de três anos após a eliminação dos *logs.*

A informação tratada é recolhida de forma lícita (cfr. alínea a) do n.º 1 do artigo 5.º da LPD), para finalidades determinadas, explícitas e legítimas (cfr. alínea b) do mesmo artigo) e não é excessiva.

III. Da Conclusão

Assim, de acordo com o disposto no n.º 2 do artigo 7.º, alínea a) do n.º 1 do artigo 28.º e n.º 1 do artigo 30.º da Lei de Protecção de Dados, autoriza-se o tratamento nos seguintes termos e com as seguintes condições:
Responsável pelo tratamento: Clínica CUF Belém, S.A.
Finalidade: Disponibilização aos utentes, através da Internet, de resultados/relatórios de meios complementares de diagnóstico, do histórico de consultas e exames realizados e possibilidade de marcação de consultas (serviço MyCUF).

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Categoria de Dados pessoais tratados: nome, telefone, correio eletrónico, data de nascimento, username e palavra-chave, logs e IP de acesso, unidade em que pretende a consulta/exame, especialidade, ato médico, médico para que pretende marcar o episódio médico, data e hora da marcação, entidade financeira responsável pelo pagamento, observações indicadas pelo utilizador, digitalização submetida pelo utilizador, n.º de cliente (para clientes autenticados), nome, data de nascimento, telefone e correio eletrónico (para clientes não registados), especialidade, ato e rúbrica do episódio realizado, unidade de saúde em que se realizou, data de início e fim do episódio, estado do episódio, profissional de saúde que executou o episódio, n.º de episódio, tipo de episódio, indicação se existem resultados do episódio e identificador desses resultados, n.º de cliente que realizou o episódio.

Entidades a quem podem ser comunicados: Não há.

Formas de exercício do direito de acesso e retificação: Junto da responsável pelo tratamento.

Interconexões de tratamentos: Não há.

Transferências de dados para países terceiros: Não há.

Prazo de conservação:

a) **Dados de saúde** – Nos termos do anexo à Portaria n.º 247/2000, de 8 de Maio;

b) ***Logs* de acesso** – 2 anos.

Da presente Autorização decorrem obrigações que o responsável deve cumprir. Deve, igualmente, dar conhecimento dessas condições a todos os intervenientes no circuito de informação.

Lisboa, 09 de julho de 2013

Carlos Campos Lobo (Relator), Luís Barroso, Ana Roque, Helena António, Vasco Almeida, Luís Paiva de Andrade

Filipa Calvão (Presidente)

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

DECLARAÇÃO DE VOTO

Processos nºs 6219/2012, 6551/2012, 6221/2012, 6220/2012, 6653/2012, 6222/2012, 6223/2012, 6550/2012

Esta declaração de discordância incide apenas sobre o ponto I, Secção E, "Da Subcontratação dos Serviços". Em meu entender, no caso do contrato celebrado com a ONI – Telecom – Infocomunicações, S. A., para instalação dos servidores da José de Mello Saúde no centro de dados da ONI, esta empresa não se encontra autorizada, nos termos contratuais, para tratar dados pessoais por conta da JMS, pelo que não deve ser qualificada como subcontratante, para efeitos da aplicação do artigo 14º da Lei nº 67/98, de 26 de outubro, nesta secção da autorização.

Se, ainda assim, a situação de controlo de facto sobre os servidores propiciar a ocorrência de qualquer tratamento de dados pessoais, estaremos, porventura, perante uma violação das regras sobre proteção de dados, sancionável pela Lei nº 67/98, mas não especificamente face à violação dos deveres de uma subcontratação assumida contratualmente.

O vogal da CNPD

Vasco Almeida

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt