<http://spms.min-saude.pt/seguranca-da-informacao/>

Associado ao crescente entusiasmo relacionado com a transformação digital emerge também a preocupação com os riscos relacionados com a tecnologia. A transformação digital requer a gestão dos riscos tecnológicos, pois obriga as organizações a ter em consideração as Boas Práticas e a controlar as implementações.

A cibersegurança será o principal desafio para as instituições hospitalares uma vez que o número de ameaças bem-sucedidas nestas instituições cresceu significativamente nos últimos meses. Sabe-se que, nos Estados Unidos, mais de 110 milhões de registos individuais de saúde foram alvo de ciber-ataques em instituições hospitalares; facto que representa um número 3 vezes superior de indivíduos afetados quando comparado com o total de ameaças ocorridas entre 2009 e 2014.

Um em cada três consumidores encontram-se em risco de ter os seus registos de saúde violados, sendo  crescentemente expostos ao roubo da sua identidade financeira  e ao roubo de identidade médica. Segundo um estudo da Medical Identity Theft Alliance (MIFA), o roubo de identidades médicas cresceu cerca de 22%, podendo este número ser superior.

Os ciber-criminosos estão a tornar-se mais sofisticados nos seus ataques, levando a um aumento de ameaças em número e em alcance no sector da saúde, devido à perceção destas instituições serem um alvo fácil. No passado, as intromissões ocorriam através de ataques massivos de phishing, utilizando, frequentemente para o efeito, mensagens de correio eletrónico amplamente distribuídas com links maliciosos ou com um anexo que introduzia malware na organização. Presentemente, os ataques de phishing são mais específicos e direcionados (spear phishing e whaling), envolvendo a engenharia social para aceder às credenciais. Os ciber-criminosos aperfeiçoaram também o envio de mensagens de correio eletrónico, tornando-as semelhantes às de fontes legítimas ex.: departamento de TIC das instituições hospitalares, instituições financeiras e outras fontes de instituições fidedignas.

(As ameaças de ransomware, que encriptam ficheiros críticos do sistema tornando-os inacessíveis até que um resgate seja pago, constituem uma ameaça considerável às organizações. O impacto do ransomware vai muito para além da extorsão de dinheiro, pois poderão afetar os cuidados de saúde, as operações diárias e a segurança dos doentes. Quando os sistemas vitais são bloqueados, as equipas têm de recorrer a processos manuais e em papel, o que pode criar atrasos no acesso a informação crítica sobre os doentes e, deste modo, causar atrasos na prestação de cuidados de saúde. Em casos extremos, os hospitais afetados por este tipo de ataques transferiram doentes para outros hospitais e cancelaram agendamentos, por não terem acesso aos registos médicos.)

Prevê-se que, futuramente, os ataques passem a explorar as vulnerabilidades dos softwares associados a equipamentos médicos que se encontrem ligados à rede e interconectados a tecnologias de informação da saúde.

um relatório recente evidencia que equipamentos como bombas de insulina, monitores cardíacos e sistemas PACS têm sido utilizados por ciber-criminosos como um meio de criar uma backdoor e aceder às redes das instituições de cuidados de saúde.

Neste contexto, as instituições governamentais, a nível central e local, encontram-se pressionadas a proteger os seus sistemas de TIC e os respetivos dados de todas as formas de ciber-ataques.

A SPMS desenvolveu o **IT Security Assessment** de Segurança TIC na Administração Pública para auxiliar e dar suporte aos administradores governamentais, responsáveis de TIC e responsáveis departamentais na compreensão da magnitude das ameaças e das mudanças necessárias para proteger os seus organismos e os seus programas de atuação.  Esta ferramenta consiste numa framework com cinco dimensões — visão, gestão de risco, pessoas, processos e tecnologias de segurança.

<http://www.idcspms.pt/inquerito/idcquest/index.php>

A segurança de TI é um conceito generalizado no sector privado. A maioria das empresas privadas, como as do sector financeiro, de energia, de distribuição e outros sectores têm sido alvos de ciber-ameaças que variam desde o malware até roubo de propriedade industrial e 'ransomware'. Todos estes sectores que foram confrontados com estas ameaças implementaram tecnologias como firewalls, encriptação e outras para proteger a organização e os seus dados. No entanto, e apesar desta realidade em que as empresas privadas têm vindo a desenvolver esforços para proteger os seus sistemas e os seu ativos digitais, as instituições de saúde e governamentais permanecem atrasados relativamente ao sector privado. Existem algumas exceções, como o caso das entidades militares, de defesa ou de inteligência e de segurança pública, principalmente porque estas organizações enfrentam ameaças externas e internas há muitos anos.

Neste contexto, a SPMS disponibiliza aqui uma ferramenta, com base no modelo internacional da IDC "MaturityScape IT Security”,  para auxiliar e dar suporte aos administradores governamentais, responsáveis de TIC e responsáveis departamentais na compreensão da magnitude das ameaças e das mudanças necessárias para proteger os organismos governamentais e os seus programas de atuação.  Esta ferramenta consiste numa framework com cinco dimensões — visão, gestão de risco, pessoas, processos e tecnologias de segurança.

<http://spms.min-saude.pt/transformacao-digital/>

O sector da saúde é caraterizado pelas seguintes tendências:

•Dados e informação sobre doentes é recolhida através de uma vasta quantidade de sistemas de TIC e de equipamentos médicos. Frequentemente, não existe ou existe pouco conhecimento sobre o armazenamento dos dados dos pacientes.

•As vias de tratamento são criadas através do ecossistema do doente num ambiente de cuidados integrados, no qual todos os prestadores de serviços, incluindo os doentes, têm acesso aos dados. Tais podem ser soluções de telemedicina ou plataformas de cuidados partilhados.

•O tratamento moderno de doentes está fortemente dependente de dados e de informação, como a medicina de precisão ou as vias de cuidados pessoais.

•Dados e informação são partilhados para outros objetivos que não o tratamento direto dos mesmos. Tal poderá ser para investigação, gestão de saúde pública ou gestão da procura através dos sectores.

•Dados e informação são utilizados conjuntamente com analítica, Big Data e sistemas cognitivos para permitir novos regimes de tratamento e novos modelos de negócio.

<http://spms.min-saude.pt/alertas-e-seguranca/>

No início de 2016, variantes destrutivas de ransomware como o Locky ou o Samas infetaram computadores individuais e de empresas, em estabelecimentos de saúde e hospitais em todo o mundo. O Ransomware é um tipo de software malicioso que infecta um computador e restringe o acesso dos utilizadores até que uma quantia de dinheiro seja paga para o desbloquear.

O Ransomware é um tipo de malware que infecta os sistemas de computadores, restringindo o acesso dos utilizadores aos sistemas infetados. Ao longo de vários anos tem-se observado que diversas variantes de ransomware muitas vezes exibem um alerta no ecrã para tentar extorquir dinheiro das vítimas. Normalmente, esses alertas indicam ao utilizador que os seus sistemas foram bloqueados ou que os seus arquivos foram encriptados. Os utilizadores são informados de que, a menos que uma quantia seja paga, o acesso aos mesmos não será restabelecido. O montante exigido aos indivíduos varia muito, mas é frequentemente entre 200€ e 400€ euros e deve ser pago em moeda virtual, como o Bitcoin.  
O Ransomware é frequentemente transmitido através de e-mails phishing que contêm anexos maliciosos ou através de drive-by download. O drive-by download ocorre quando um utilizador visita um site infetado e, em seguida, o malware é transferido e instalado sem o conhecimento do mesmo  
O Ransomware Crypto, uma variante do malware que encripta ficheiros, é difundido através de métodos semelhantes aos mencionados sendo também difundido através de redes sociais, como aplicações de mensagens instantâneas. Além disso, novos métodos de infeção via ransomware têm sido observados. Por exemplo, servidores vulneráveis da Web têm sido analisados como um ponto de entrada para obter acesso à rede de uma organização.

Os autores de *ransomware* impregnam medo e pânico nas suas vítimas, o que faz com que estas cliquem num *link* ou paguem uma quantia de dinheiro, e consequentemente os sistemas podem ficar infetados com *malware* adicional. O *ransomware* exibe mensagens intimidadoras semelhantes às seguintes:

•“O seu computador foi infetado com um vírus. Clique aqui para resolver o problema. “

•“O seu computador foi usado para visitar *websites* com conteúdo ilegal. Para o desbloquear, deve pagar uma multa de 100€. “

•“Todos os arquivos no seu computador foram encriptados. Deve pagar este montante dentro de 72 horas para recuperar o acesso aos seus dados. “

Em 2012, a Symantec, utilizando dados de um servidor de comando e controle (C2) de 5.700 computadores comprometidos num dia, estimou que aproximadamente 2,9% dos utilizadores comprometidos pagaram a quantia requerida. Com um montante médio de 200€ os atores mal-intencionados lucraram 33.600€ por dia, ou 394.400€ por mês, a partir de um único servidor C2. Estas estimativas aproximadas demonstram como o ransomware pode ser lucrativo.  
Este sucesso financeiro levou provavelmente a uma proliferação das várias variantes de ransomware. Em 2013, as variantes mais destrutivas e lucrativas foram introduzidas, incluindo Xorist, CryptorBit e CryptoLocker. Algumas variantes encriptam não só os ficheiros no dispositivo infetado, mas também o conteúdo de unidades compartilhadas ou em rede. Essas variantes são consideradas destrutivas porque encriptam documentos de utilizadores e organizações tornando-os inúteis (inacessíveis) até que os criminosos recebam o dinheiro.  
No início de 2016, a variante destrutiva de ransomware – Locky, infetou computadores pertencentes a instalações de saúde e hospitais nos Estados Unidos, Nova Zelândia e Alemanha. Este tipo de ransomware propaga-se através de e-mails de spam que incluem documentos Microsoft Office maliciosos ou anexos comprimidos (por exemplo, ficheiros com formato .rar, .zip). Os anexos maliciosos contêm macros ou documentos JavaScript que transferem arquivos Ransomware-Locky.  
O Samas é outra variante destrutiva de ransomware e foi usada para comprometer as redes de instalações de saúde em 2016. Ao contrário do Locky, o Samas propaga-se através de servidores vulneráveis da Web. Depois do servidor Web ter sido comprometido, os ficheiros Ransomware-Samas transferidos são usados para infetar as redes da organização.

Impacto

as empresas também podem ser infetadas por *ransomware*, levando a consequências negativas, incluindo:

•Perda temporária ou permanente de informações proprietárias ou confidenciais;

•Disrupção de operações regulares;

•Perdas financeiras para restaurar sistemas e arquivos.

•Potencial danos da reputação de uma organização.

Pagar o montante solicitado não garante que os arquivos encriptados sejam disponibilizados; apenas garante que os atores maliciosos recebem o dinheiro da vítima e, em alguns casos, as suas informações bancárias. Além disso, desencriptar ficheiros não significa que o *malware* em si tenha sido removido.

Solução

Estes ataques que infetam os computadores podem ser devastadores para organização, e a recuperação pode ser um processo difícil que pode exigir os serviços de um especialista em recuperação de dados.bn 3   
O *CSIRT-eSIS* recomenda que os utilizadores e administradores tomem as seguintes medidas preventivas para proteger as suas redes de computadores de *ransomware*:

•Utilizar um *backup* de dados e um plano de recuperação para todas as informações críticas. Executar e testar *backups* regulares para limitar o impacto das perdas de dados ou sistemas e para acelerar o processo de recuperação. Analisar que os *backups* conectados em rede também podem ser afetados pelo *ransomware*; *Backups* críticos devem ser isolados da rede para uma proteção ótima.

•Utilizar a aplicação *whitelisting* para ajudar a prevenir que programas maliciosos e programas não aprovados sejam executados. A aplicação *whitelisting* é uma das melhores estratégias de segurança, pois permite que apenas os programas especificados sejam executados, bloqueando todos os outros, incluindo *softwares* maliciosos.

•Manter o seu sistema operacional e os *softwares* atualizados com os *patches* mais recentes. Aplicações e sistemas operacionais vulneráveis são alvos da maioria dos ataques. Assegurar que estas sejam *patched* com as atualizações mais recentes reduz bastante o número de pontos de entrada disponíveis para serem exploradas por um atacante.

•Manter o *software* de antivírus atualizado e que faça um *scan* de todo o *software* transferido da Internet antes da sua execução.

•Restringir a capacidade dos utilizadores (permissões) para instalar e executar aplicações de *software* indesejadas e aplicar o princípio de “Privilégio mínimo” a todos os sistemas e serviços. Restringir esses privilégios pode prevenir que seja executado *malware* ou limitar a sua capacidade de se difundir pela rede.

•Evitar a ativação de macros de anexos de *e-mail*. Se um utilizador abrir o anexo e permitir macros, o código incorporado executará o *malware* no dispositivo. Para empresas ou organizações, pode ser melhor bloquear mensagens de *e-mail* com anexos de fontes suspeitas.

•Não clicar em*links* não solicitados em *e-mails*.

**O que é um ataque phishing?**

O phishing é uma forma de engenharia social. Os ataques phishing usam e-mails ou sites maliciosos para solicitar informações pessoais, posicionando-se como uma organização confiável. Por exemplo, um atacante pode enviar um e-mail que aparentemente é de uma empresa de cartão de crédito respeitável ou de uma instituição financeira que solicita informações de conta, muitas vezes sugerindo que há um problema. Quando os utilizadores respondem com as informações solicitadas, os atacantes podem usá-las para obter acesso às suas contas.

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

## ****RSE – Registo de Saúde Electrónico****

O Registo de Saúde Electrónico (RSE) – visa a reunir informação essencial de cada Cidadão para a melhoria da prestação de cuidados de saúde; o RSE é construído por dados clínicos recolhidos electronicamente para cada Cidadão e produzidos por entidades que prestam cuidados de saúde.

O RSE permite o registo e partilha de informação clínica entre o utente, profissionais de saúde e entidades prestadoras de serviços de Saúde, de acordo com os requisitos da Comissão Nacional de Proteção de Dados (Autorização n.º 940/2013).

É constituída por quatro portais, seguros e contextualizados: Área do Cidadão; Portal do Profissional; Portal Institucional e Portal Internacional.

**RSE – Área do Cidadão**

Portal lançado em maio de 2012, destinado aos utentes com o objetivo de melhorar a qualidade dos serviços prestados. Na secção **“A minha saúde”** o utente passa a ter um papel ativo na manutenção, promoção e melhoria do seu estado de saúde e, consequentemente, um atendimento mais eficaz e seguro.

**Serviços eletrónicos disponíveis mediante autenticação no portal:**

* Registo de **contactos de emergência**
* Registo de informação sobre **hábitos, medicação, alergias e doenças**
* Registo das medições de **peso, altura, glicémia, tensão arterial, colesterol, triglicéridos, saturação de oxigénio e de tempo de coagulação do sangue**(INR)
* Carregamento de **documentos de saúde**, como análises clínicas, relatórios médicos e similares
* **Partilha dos dados de saúde com os profissionais de saúde do SNS**(hospitais, urgências, cuidados de saúde primários), mediante autorização prévia do utente, e com a possibilidade de poder consultar o histórico de acessos a essa informação
* **Contacto direto com o seu centro de saúde**(administrativo, enfermeiro ou médico)
* **Marcação online de consultas**médicas para os prestadores de Cuidados de Saúde Primários do SNS;
* **Pedido de prescrição de medicação crónica**prevista na lista de medicamentos autorizados pelo médico do prestador de cuidados de saúde primários do SNS;
* Associação do seu **agregado familiar**, possibilitando a realização de marcações de consulta médica e pedidos de prescrição de medicação crónica para os seus familiares;
* Consulta da situação da inscrição, a posição na lista e o tempo de espera previsível para cirurgia por parte dos utentes do SNS inscritos para cirurgia através da aplicação **eSIGIC**;
* Preenchimento e submissão de **pedidos de isenção do pagamento das taxas moderadoras**, bem como a consulta do estado do pedido e a reclamação sobre o resultado obtido.
* Consulta do cronograma referente ao **historial clínico**;

**Serviços eletrónicos disponíveis mediante autenticação com Cartão de Cidadão no portal:**

* Consulta do **eBoletim de Saúde Infantil e Juvenil**(marcações de consultas, reforço de vacinas ou a realização de exames clínicos, entre outros);

Consulta dos **dados que constam do Resumo Clínico Único** (RCU): alergias, medicação, diagnósticos, cirurgias e vacinação.

**RSE – Portal do Profissional**

Consiste numa plataforma **centrada no utente** que permite aos profissionais de saúde (médicos e enfermeiros) terem **acesso à informação clínica do utente**.

Desde o seu lançamento, em junho de 2012, já conta com mais de 530 instituições, incluindo todos os CS e todos os hospitais do SNS.

A informação que o utente disponibiliza na Área do Cidadão e que, posteriormente, autoriza a sua consulta, permite ao profissional de saúde obter alguns indicadores que o podem auxiliar a um **melhor conhecimento, diagnóstico e tratamento** do mesmo.

Para além do acesso ao processo clínico eletrónico do utente, são também disponibilizadas as seguintes funcionalidades:

* Cronograma com todos os contactos efetuados pelo utente, nas diversas instituições do país. Os tipos de contactos disponibilizados nesta fase são:
  + INEM
  + Saúde Oral
  + Saúde 24
  + RNCCI – Rede Nacional de Cuidados Continuados Integrados
  + GID – Doença renal crónica
  + BDMP – Repositório nacional de prescrições
* Informação partilhada pelo utente na Área do Cidadão:
  + Contactos de urgência
  + Dados de saúde
  + Hábitos
  + Medicação
  + Alergias
  + Doenças
* Resumo de Saúde Oral:
  + História Clínica e detalhes dos contactos
  + Diagnósticos e tratamentos orais
  + Diagnósticos e tratamentos dentários
* Visualização das prescrições de medicamentos emitidas

MUITO ARRISCADO:

Existe também uma versão do Portal do Profissional disponível para acesso pelos médicos a titulo individual. Nesta versão o profissional poderá aceder e beneficiar de um conjunto de funcionalidades e serviços, bastando para isso pedir acesso através do formulário disponível – (<http://spms.min-saude.pt/plataforma-dados-saude-titulo-individual/>)

**RSE – Portal Institucional**

Disponibilização de **backoffice** para gestão centralizada do RSE e **estatísticas** referentes ao RSE. Prevê-se a criação de um repositório de informação clínica anonimizada, residente na DGS, para fins de **saúde pública** e **investigação epidemiológica**.

**RSE – Portal Internacional**

Por intermédio do projeto europeu **epSOS**, a RSE permite que um médico de outro país da União Europeia consulte o **Resumo Clínico Único** do utente, mediante a sua autorização prévia no portal.

**Exemplo de um acontecimento:**

<https://gauchazh.clicrbs.com.br/geral/noticia/2017/02/dados-vazados-sobre-estado-de-saude-de-marisa-leticia-abrem-debate-sobre-etica-medica-9713064.html>

Dados vazados sobre estado de saúde de Marisa Letícia abrem debate sobre ética médica

### **[Caso recente: 04/02/2017]**

### Informações sigilosas do diagnóstico da ex-primeira-dama Marisa Letícia tornaram-se públicas após conversa em grupo no WhatsApp

**O vazamento, em um grupo de Whatsapp, de informações sobre o estado de saúde da ex-primeira-dama Marisa Letícia Lula da Silva** reacendeu o debate sobre como médicos lidam com o sigilo em ambientes digitais. Por ter enviado mensagens a ex-colegas de faculdade em que confirmava o diagnóstico de Marisa Letícia – respondendo a um médico que publicou uma imagem de um exame da mulher de Lula –, a reumatologista Gabriela Munhoz, 31 anos, foi demitida do Hospital Sírio-Libanês, em São Paulo, e é alvo de sindicância aberta pelo Conselho Regional de Medicina do Estado de São Paulo (Cremesp).

O presidente do Cremers, Fernando Mattos, alerta para o perigo de tratar desse tipo de informação nesse meio:

– A divulgação dos dados pessoais, mesmo em caráter privado, deve ser evitado. Às vezes, a gente comenta alguma coisa com a mulher, com alguém muito próximo. O cuidado do médico tem de ser bem maior quando se trata de redes sociais. Há uma difusão muito rápida. É um grupo de amigos que tem acesso, não só aquele mais próximo. Quando fala com um, os outros ficam sabendo. A partir daí, há uma divulgação em cadeia.

Presidente da Associação Brasileira de Medicina, Florentino Cardoso acredita que há um aumento nos casos de vazamentos a partir do advento de meios digitais como o WhatsApp. Lembra, porém, que a recomendação segue a de manter sigilo total sobre informações de pacientes.

– O sigilo é sagrado. Estas informações não podem estar circulando. Tem de respeitar a privacidade do doente. Não há diferença nenhuma na orientação que sempre se deu. Cada vez mais aparecem recomendações para se ter muito cuidado nas redes sociais. Temos visto mais casos assim, ainda que esse aumento não tenha sido mensurado. Temos de considerar, também, que as redes sociais possibilitam fakes, montagens. Não se sabe se a informação é fidedigna – analisa.

Segundo o presidente do Conselho Regional de Medicina do Estado de São Paulo (Cremesp), Mauro Aranha:

“ a questão do vazamento de exames, prontuarios ou qualquer coisa que revele a doença pela qual a pessoa está passando fere o sigilo médico, fere frontalmente o artigo 73 do código de ética médica, que se refere à quebra do sigilo. E comentários desabonadores da parte de um médido ferem o artigo 23, que trata da dignidade do paciente, que fala sobre nenhuma forma de discriminação de uma pessoa doente e que dependa da benemerência e da qualidade do atendimento por aquele médico. Muitos médicos têm procurado o conselho, ou comentado por redes sociais, pedindo providências. (casos como esse) São uma exceção, mas uma exceção que tem crescido, e isso nos preocupa.”

“Apuramos fatos. Foram dois fatos. A quebra de sigilo e, em uma outra situação, os comentários desonrosos por parte de médicos nas redes sociais sobre uma pessoa doente. Nós sindicamos o fato. Significa buscar indícios de infração a artigos do código de ética médica e quem cometeu estas eventuais infrações. A partir disso, abre-se o processo para cada um dos envolvidos. Ao fim, é julgado e se estabelecem as penas, para quem for culpabilizado.”

**Outros profissionais que fizeram comentários em redes sociais, grupos de WhatsApp, também podem ser responsabilizados?**

“Quando falamos de um médico x, temos que ter uma razoável aproximação de que este médico fez aquele comentário. Essa pessoa falou para alguém, que também pode ser médico e eventualmente respondeu cometendo uma possível infração ética.”

**E no caso específico da médica do Sírio-Libanês?**

“Abrimos a sindicância e enviamos ofício para que as partes envolvidas. Todos terão de vir ao conselho responder a isso.”

“O rito é a instrução da sindicância, que pela gravidade da questão será feita da forma mais célere possível. A partir daí abre-se ou não o processo ético-profissional e vem o julgamento. Não é um processo rápido. E nem pode ser algo que não atenda aos dispositivos legais de direito ao contraditório. Temos que fazer com responsabilidade. Em média, pode demorar de dois a cinco anos. Mas casos que envolvem situações mais graves procuramos ao menos na fase da sindicância dar uma celeridade maior.”

**Quais são as punições possíveis para este caso, caso comprovada culpa?**

“Temos cinco penas: advertência confidencial, censura confidencial, censura pública em jornal de grande circulação, suspensão por até 30 dias e cassação do exercício profissional. Cassação também precisa passar pelo Conselho Federal de Medicina.”

**O que diz o Código de Ética**

“De acordo com o Código de Ética Médica, é vedado ao médico "permitir o manuseio e o conhecimento dos prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade". Também não é permitido "liberar cópias do prontuário sob sua guarda, salvo quando autorizado, por escrito, pelo paciente, para atender ordem judicial ou para a sua própria defesa", esta última em situação de sindicância ou processo ético-profissional. No cenário de doentes "notáveis", a informação para o público deve ocorrer por meio de boletim médico autorizado pelo paciente ou responsável.”

**Contexto**

Em 24 de janeiro, Marisa Letícia passou mal em casa, em São Bernardo do Campo (SP). Ela foi levada inicialmente para o Hospital Assunção, na mesma cidade. De lá, foi levada para o Sírio-Libanês, em São Paulo, onde chegou com diagnóstico de acidente vascular cerebral (AVC). Ela foi levada diretamente para o setor de emergência. Os médicos sedaram e colocaram a ex-primeira-dama em um respirador mecânico.

Horas depois da internação, a médica reumatologista Gabriela Munhoz, 31 anos, enviou mensagens a um grupo de WhatsApp de antigos colegas de faculdade, confirmando que Marisa Letícia estava no pronto-socorro com diagnóstico de [**AVC hemorrágico**](http://zh.clicrbs.com.br/rs/vida-e-estilo/vida/noticia/2016/03/avc-sintomas-prevencao-e-tratamentos-5115257.html).

A mensagem foi compartilhada no grupo "MED IX" e se espalhou em outros grupos de WhatsApp.

um outro médico de fora do Sírio-Libanês postou no grupo imagens de uma tomografia atribuída a Marisa Letícia, acompanhada de detalhes que foram confirmados, em seguida, pela médica reumatologista. As informações foram compartilhadas em outro grupo de médicos, intitulado "PS Engenho 3", e atribuídas a um cardiologista. Quando a médica diz que Marisa Letícia ainda não tinha sido levada para a UTI, um colega residente em urologia dispara: "Ainda bem!".

A médica responde com risadas. Outro médico do grupo, um neurocirurgião, também ironizou o quadro de dona Marisa: "Esses fdp vão embolizar ainda por cima", escreveu. O procedimento de embolização provoca o fechamento de um vaso sanguíneo para diminuir o fluxo de sangue em determinado local. "Tem que romper no procedimento. Daí já abre pupila. E o capeta abraça ela", escreveu o médico.

Gabriela foi demitida e é alvo de sindicância do Cremesp. Uma investigação interna foi aberta, também, no Hospital Assunção, em São Bernardo do Campo.

<https://gauchazh.clicrbs.com.br/geral/noticia/2017/02/marisa-leticia-teve-dados-sigilosos-de-diagnostico-vazados-por-medica-do-sirio-libanes-9708333.html>

# Marisa Letícia teve dados sigilosos de diagnóstico vazados por médica do Sírio-Libanês

Os dados foram compartilhados em um grupo de WhatsApp poucas horas após a entrada da mulher do ex-presidente Lula na casa de saúde. As informações são do jornal [**O Globo**](http://oglobo.globo.com/brasil/medica-do-sirio-compartilhou-dados-sigilosos-do-diagnostico-de-marisa-20864217).

Ela enviou os documentos para um grupo de amigos de faculdade, liberando diversas informações sobre a internação de Marisa Letícia e o estado de saúde dela na data. A conduta é ilegal, visto que o Código de Ética Médica deixa claro que profissionais da área da saúde não podem divulgar para terceiros prontuários de pacientes.

No Capítulo IX do Código de Ética Médica disponível no site do Conselho Federal de Medicina, o artigo 73 deixa claro que é vedado ao médico "revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente" e que a proibição permanece "mesmo que o fato seja de conhecimento público".

Após esse primeiro vazamento, os arquivos se espalharam nas redes sociais, inclusive com informações que não constavam no boletim divulgado oficialmente pelo hospital, horas depois. No mesmo grupo no qual a reumatologista enviou os dados, outro médico enviou imagens de tomografia atribuída a Marisa Letícia.

<https://www.computerworld.com.pt/2017/03/23/desafios-da-gestao-da-informacao-na-saude/>

<http://portal-chsj.min-saude.pt/pages/716>