Instituto Português da Qualidade

Comissão Setorial para a CS/09 Saúde

REGISTO DE SAÚDE ELETRÓNICO

RECOMENDAÇÕES DA CS/09
PARA A CERTIFICAÇÃO DO *SOFTWARE*
DO REGISTO DE SAÚDE ELETRÓNICO (RSE)

(REC CS09/03/2024)

Registo de Saúde Eletrónico
(REC CS09/03/2024)

Instituto Português da Qualidade | Ministério da Economia
Comissão Setorial para Saúde (CS/09)

1.ª Edição
Instituto Português da Qualidade | julho 2024

Rua António Gião, 2
2825-513 CAPARICA
PORTUGAL
Tel: +351 212 948 100
email: ipq@ipq.pt
www.ipq.pt

Autores

CS/09 – GT5 – Sistemas de Informação em Saúde
Elisabete Melo Gomes
Mário Macedo

Coordenação

Mário Macedo

ISBN 978-972-763-188-9

ÍNDICE

INTRODUÇÃO

O Registo de Saúde Eletrónico (RSE) é definido como um repositório de informação sobre saúde de indivíduos e populações, recolhida de forma sistematizada e longitudinal, armazenada e transmitida de forma segura em formato digital e acessível em tempo real a pessoas autorizadas.

A segurança dos dados individuais de saúde obtém-se com o desenho adequado do *software* do RSE, cumprindo protocolos definidos em normas internacionais e na legislação nacional.

Uma das garantias de que o RSE cumpre a legislação, as normas técnicas e a regulamentação relativa à normalização da qualidade e da segurança, para além de auditorias de verificação, é dada através da certificação do respetivo *software,* assegurando a finalidade primária do RSE, que é, o suporte a cuidados de saúde integrados, de forma facilitada e contínua, com qualidade, efetividade e segurança.

Dada a evolução atual, os desafios, ameaças e exigências, que têm surgido ao longo dos anos, o propósito deste texto é dar uma breve informação sobre a certificação do *software* do RSE, apontando recomendações para que se torne seguro e confiável.

CONTEXTO E EVOLUÇÃO DOS REGISTOS DE SAÚDE ELETRÓNICOS

Desde os primeiros registos de dados de saúde em formato digital nos anos 60[1], e na década seguinte[2], a evolução tem sido grande.

No início dos anos 90, houve uma onda de inovação com o desenvolvimento e implementação de RSE que, à medida que se generalizaram, apresentaram alguns riscos de funcionamento e preocupações relativas à segurança e privacidade.

Na sequência da resolução de constrangimentos e de exigências relativas a acessibilidade e segurança, houve um desenvolvimento acentuado das tecnologias de informação e aplicação de medidas de cibersegurança.

A implementação de RSE foi um passo significativo no sentido da modernização das práticas de saúde em todo o mundo. Com a propagação da *internet* e o surgimento dos arquivos em *cloud,* os RSE evoluíram permitindo a ligação a outros sistemas, não apenas administrativos, financeiros ou a dispositivos de monitorização à distância, mas também a sistemas de suporte à decisão clínica, nomeadamente, com alertas automáticos, por exemplo, no caso de alergias ou interações medicamentosas. Os RSE tornaram possível o acesso do utente ao seu processo clínico digital, o que deu origem ao portal do utente, permitindo o acesso às requisições e prescrições clínicas, aos exames complementares de diagnóstico, marcação de consultas e a comunicação remota com os seus médicos, com consequente melhoria dos cuidados de saúde percecionados[3]. Esta evolução tornou evidente a necessidade de compatibilidade e interoperabilidade entre diferentes sistemas, com o desenvolvimento de protocolos seguros de partilha de dados.

Os desafios iniciais resultantes de muitas fontes heterogéneas e formatos não interoperáveis, grandes volumes de dados não estruturados, diferentes ontologias informáticas e resistência à mudança, muitas vezes por *software* de utilização não intuitiva, têm vindo a ser ultrapassados pouco a pouco.

A crescente abordagem dos cuidados de saúde centrada no cidadão e nos seus direitos, levaram a uma mudança de paradigma e à preocupação com a privacidade e segurança, surgindo, no final dos anos 90, as primeiras normas técnicas e de proteção da informação de saúde dos cidadãos e a regulamentação do acesso por parte dos prestadores de cuidados de saúde a essa informação[4]. Esta regulamentação levou à normalização dos formatos dos dados, assim como melhorou a segurança dos protocolos. A partir daí, a certificação do *software* dos RSE tornou-se um requisito essencial, assegurando o cumprimento dessas normas e regulamentações.

Os RSE continuam em constante evolução[5], apresentando presentemente muitas vantagens, ao concentrar os dados de saúde dos cidadãos num único local de rápido acesso, minimizando erros e evitando repetições que poupam tempo e recursos e permitindo em anos recentes a gestão de saúde pública, a telemedicina e a aplicação de algoritmos de inteligência artificial e tecnologias de *machine learning,* com a avaliação de grande número de dados clínicos. Estes avanços dão a possibilidade de fazer melhores diagnósticos, identificar padrões de saúde que permitam prever e prevenir determinados problemas de saúde, particularmente importantes em contextos de pandemia.

Presentemente os desafios que se colocam são a cibersegurança, a interoperabilidade entre diferentes sistemas e a proteção e privacidade dos dados de saúde, havendo a necessidade de um equilíbrio entre a acessibilidade e a privacidade.

SITUAÇÃO EM PORTUGAL COMO MEMBRO DA UNIÃO EUROPEIA

Em Portugal, existem múltiplos sistemas de informação com registos de dados de saúde dos utentes, que frequentemente não são interoperáveis. As realidades em relação a infraestruturas, nomeadamente a adequação de *hardware* e acesso à rede e conectividade com a *internet*, são díspares.

Os Serviços Partilhados do Ministério da Saúde, E.P.E. (SPMS, E.P.E.)[6], que gerem as tecnologias de informação na saúde desde 2010, têm vindo a reformular esta situação no setor público, sob a supervisão da Administração Central do Sistema de Saúde, I.P. (ACSS, I.P.). Desde 2022, a Direção Executiva do Serviço Nacional de Saúde, I.P. tem como atribuições definir, conjuntamente com a ACSS, I.P., as prioridades e respostas a assegurar pelos sistemas de informação e comunicação a fornecer pela SPMS, E.P.E., mediante contratos-programa[7].

Será necessário garantir a qualidade das soluções e criar um ecossistema de desenvolvimento tecnológico, dinamizando a produção tecnológica por via da normalização e abertura de mercado e promover a formação e treino de profissionais. Será necessário também promover a literacia digital, de forma a todos terem acesso, de acordo com o respetivo perfil de utilizador.

Em 2023, os SPMS, E.P.E. anunciaram a intenção de implementar um RSE único, que permita a compatibilidade e interoperabilidade entre o sistema privado e o Serviço Nacional de Saúde (SNS).

Esta abordagem está em consonância com a política da União Europeia, que tem vindo a promover a transformação digital na saúde e a interajuda entre Estados-Membros no campo da cibersegurança, promovendo também a existência de RSE nacionais baseados num formato comum e seguro de troca de informação de saúde, que permitam uma acessibilidade pelos profissionais de saúde autorizados aos dados de saúde dos cidadãos na Europa, de forma a obter diagnósticos e tratamentos mais rápidos.

Existem na Europa organizações que promovem a existência de RSE eficientes que cumpram os critérios da qualidade, segurança, privacidade, funcionalidade e interoperabilidade entre diferentes sistemas de informação, e que impulsionam a certificação do respetivo *software*, que tem vindo a tornar-se de importância crescente nos últimos anos[8].

A Comissão Europeia, através da sua *eHealth legislation,* tem sido pró-ativa estabelecendo normas para RSE. Esta legislação promove a implementação por parte dos Estados-Membros de RSE certificados, utilizando uma aproximação normalizada para assegurar a interoperabilidade e partilha transfronteiriça de

dados, nomeadamente, com o projeto da *eHealth Digital Service Infrastructure* (eHDSI)[9], que estabelece uma infraestrutura para partilha de dados de saúde transfronteiriços e acesso seguro dos profissionais de saúde aos RSE, no caso de cidadãos que recebem cuidados de saúde noutro país da Europa, e mediante o consentimento explícito do titular dos dados.

Na sequência da criação do *European Health Data Space* em 2022, a União Europeia estabeleceu no seu programa Década Digital, que uma das metas digitais para 2030 é a de 100% dos cidadãos da União Europeia terem acesso aos seus registos de saúde eletrónicos (Artigo 4.º n.º 1 4) b) da Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022[10]).

CERTIFICAÇÃO DO *SOFTWARE* DO RSE

A certificação do *software* tem melhorado significativamente a eficácia dos RSE, tendo inclusivamente alguns países recorrido a incentivos para a sua promoção[11].

A certificação do *software* dos RSE é um processo que vai para além de uma simples validação que ateste a conformidade com critérios específicos. Assegura a integridade, segurança e qualidade do *software* em utilização, minimizando erros, aumenta a segurança do utente e mitiga o risco de ameaças aos dados, melhorando significativamente a adesão, a confiança e a eficácia dos RSE.

Um aspeto importante a ter em conta na certificação é a possibilidade de avaliação da usabilidade para o propósito pretendido e para o tipo de utilizador, quer para profissionais de saúde, quer para utentes na respetiva área do cidadão, pela facilidade operacional, satisfação do utilizador, flexibilidade do sistema, eficiência e efetividade, sendo conveniente a possibilidade de registo do *feedback* para posterior avaliação e implementação de melhorias.

A facilidade operacional é um motivo importante na satisfação do utilizador, que condiciona a adesão e, no caso dos profissionais de saúde, influencia a fluidez nos cuidados de saúde prestados, podendo ser um fator condicionador da dimensão económica.

Alguns dos desafios a ter em consideração são, o vocabulário normalizado, a interoperabilidade com outros sistemas e o planeamento estratégico na área dos RSE, sendo de extrema importância o levantamento das necessidades e aplicabilidade das tecnologias, ouvindo a voz dos utilizadores[12].

CRITÉRIOS DE CERTIFICAÇÃO DO *SOFTWARE* DO RSE

Os organismos reguladores governamentais definem os critérios para a certificação do *software* dos RSE, sendo critérios fundamentais para a qualidade de um RSE, os seguintes:

- Desenho centrado na facilidade de utilização e adequação ao propósito pretendido, com integração das necessidades e requisitos dos utilizadores;
- Confiabilidade e existência de um sistema de gestão de risco instalado;
- Privacidade e segurança dos dados de saúde dos utentes, identificados de forma única e inequívoca, controlo de acessos e autenticação, encriptação, rastreamento e notificação ao utente;
- Funcionalidade técnica e eficiência no desempenho, relativamente à capacidade de armazenamento de dados, segurança do sistema, interoperabilidade com outros sistemas e recurso a análise de dados;
- Mantenabilidade, o *software* deve ser de fácil manutenção e atualização;
- Portabilidade, que permita a transferência segura de dados;
- Adesão às normas da qualidade, segurança e legislação em vigor.

NORMALIZAÇÃO PARA *SOFTWARE* DO RSE

Todos os critérios, obedecem a normas da qualidade e segurança, internacionais e nacionais, bem como à legislação em vigor, com relevância para a proteção de dados, direitos dos utentes e permissões para o acesso e processamento de dados pessoais, cujo cumprimento é avaliado pelo desenho da arquitetura do *software* do RSE e por rigorosos testes de verificação e validação, no processo de certificação.

O não cumprimento dos critérios da qualidade e segurança, quer no desenvolvimento do *software* do RSE, quer na sua utilização, pode originar efeitos adversos na prestação de cuidados de saúde ao utente e colocar em risco a sua situação clínica[13].

Existem mais de duzentas normas que visam os sistemas de informação, a maior parte elaboradas pela *International Organization for Standardization* (ISO), com o qual o homólogo europeu, o *European Committee for Standardization* (*Comité Européen de Normalisation* - CEN), coopera desde 1991, pelo Acordo de Viena, com aprovação paralela das normas a nível internacional e europeu, com ganho de eficiência evitando a sua duplicação. A normalização europeia tem contribuído para a interoperabilidade das redes, desenvolvimento tecnológico e inovação[14].

A área da ISO relativa à engenharia eletrotécnica pertence à *International Electrotechnical Commission* (IEC), sendo o equivalente europeu o *European Committee for Electrotechnical Standardization/Comité Européen de Normalisation Électrotechnique* (CENELEC*),* com cooperação mútua reforçada em 2016, mediante o Acordo de Frankfurt.

Portugal, como membro participante na ISO, IEC, CEN e CENELEC através do Instituto Português da Qualidade, adota como Normas Portuguesas (NP) as normas internacionais e europeias (EN) destas organizações. Algumas normas europeias são elaboradas na sequência de um pedido de normalização por parte da Comissão Europeia, são as chamadas normas harmonizadas, ou seja, contêm especificações obrigatórias na legislação europeia.

ISO e IEC criaram em conjunto a comissão técnica, *Joint Technical Committee* (ISO/IEC JTC 1) *Information Technology*, que elabora, entre outras, as normas da série 25000, sobre qualidade (*Subcommittee SC7, Systems and software engineering*)[15] e da série 27000, sobre segurança (*Subcommittee SC27, Information security, cybersecurity and privacy protection*), sendo algumas destas normas amplamente aplicadas, apesar de generalistas[16,17].

Outras normas generalistas que se aplicam às organizações de saúde e ao RSE são as normas da série ISO 31000, que abordam o risco nas suas componentes de

identificação, análise, avaliação e controlo dos riscos, incluindo a monitorização e revisão contínuas dos processos de gestão do risco, assegurando que se mantêm atualizados e enfatizando a comunicação entre as partes interessadas, nomeadamente, organizações de saúde, utentes e autoridades reguladoras[18].

Especificamente para a tecnologia da informação na área da saúde, a comissão técnica ISO/TC 215 *Health informatics*, normaliza a tecnologia de informação e comunicação em saúde, em particular a compatibilidade e interoperabilidade entre sistemas independentes, em conjunto com as normalizações *Health Level Seven* (HL7)[19] e *Fast Healthcare Interoperability Resources* (FHIR)[20].

A representação de conceitos clínicos traduzida para informação digital, é também normalizada[21,22], sendo os dados provenientes de múltiplas fontes armazenados em formatos consistentes predeterminados, possibilitando a utilização, reutilização e interoperabilidade entre sistemas, permitindo também o suporte à decisão clínica, epidemiologia e investigação.

Para cumprimento de regras de interoperabilidade, os RSE obedecem também a normas de saúde, como a Classificação Internacional de Doenças (CID) e à normalização para a interoperabilidade semântica, utilizando a *Systematized Nomenclature of Medicine Clinical Terms* (SNOMED CT)[23]. Para codificações laboratoriais e exames clínicos com imagem e respetiva interoperabilidade, utilizam-se os *Logical Observation Identifiers Names and Codes* (LOINC)[24] e as normas DICOM (*Digital Imaging and Communication in Medicine*)[25].

SEGURANÇA E PRIVACIDADE DOS DADOS DE SAÚDE INDIVIDUAIS

A segurança dos dados individuais de saúde obtém-se com o desenho adequado do *software* do RSE, cumprindo protocolos normalizados definidos na legislação nacional e em normas internacionais, nomeadamente, no que diz respeito aos requisitos de segurança dos *softwares* em saúde durante o seu ciclo de vida[26].

Normas generalistas da qualidade e segurança, juntamente com normas específicas para RSE, que englobam, arquitetura[27], comunicação e interoperabilidade[28,29,30,31,32], incluindo a arquitetura para a interoperabilidade com outras bases de dados e aplicações previamente existentes[33], bem como, proteção dos dados de saúde individuais e gestão do risco, focam os aspetos essenciais para a confidencialidade, integridade e disponibilização segura da informação individual de saúde[34], devendo os acessos ser rastreáveis e auditáveis[35].

Uma das garantias de que o RSE cumpre a legislação, as normas técnicas e a regulamentação relativa à normalização da qualidade e da segurança, para além de auditorias de verificação, é dada através da certificação do respetivo *software*.

A certificação do *software* do RSE implica a confirmação por avaliação e verificação da existência de um sistema de gestão de risco com protocolos de segurança de forma a detetar e responder a incidentes como ciberataques, ou perda de dados não esperada, bem como, a existência de ferramentas automáticas de verificação de vulnerabilidades e de salvaguarda dos dados. A Agência da União Europeia para a Cibersegurança (ENISA: *European Union Agency for Cybersecurity*), referida no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019[36], contribui para a criação e a manutenção de um enquadramento europeu para a certificação da cibersegurança dos produtos, serviços e processos das tecnologias de informação.

O Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021[37], que cria o Programa Europa Digital reforça a implementação das tecnologias digitais avançadas, nomeadamente, a computação de alto desempenho, a cibersegurança e a Inteligência Artificial, bem como a formação nestas áreas, incluindo em matéria de proteção de dados.

A segurança em relação à proteção dos dados de saúde individuais contra o acesso não autorizado, é tão importante, quanto a cibersegurança, as capacidades e as qualidades técnicas do RSE.

Portugal segue o Regulamento Geral de Proteção de Dados (RGPD), integrado no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril

de 2016[38] e na Lei n.º 58/2019, de 8 de agosto[39], lei que assegura, na ordem jurídica nacional, o referido Regulamento.

Também no âmbito do tratamento dos dados pessoais e defesa dos direitos dos titulares desses dados, a Comissão Nacional de Proteção de Dados (CNPD) controla e fiscaliza o cumprimento do RGPD e da Lei n.º 58/2019, bem como o de outros requisitos adicionais estabelecidos pela própria CNPD, que tem autoridade para corrigir e sancionar o seu incumprimento. São considerados dados pessoais todos os dados que contêm informação que permita a identificação da pessoa singular, bem como, elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social, incluindo dados genéticos e biométricos, definidos na Lei n.º 59/2019, de 8 de agosto[40], transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016[41]. Existem regras internacionais para a recolha, utilização e descarte da informação de saúde individual[42].

O sigilo profissional e a obrigatoriedade de confidencialidade a que estão sujeitos por lei os profissionais de saúde, quer do sistema público, quer do privado, e todos os responsáveis pelo tratamento de dados (n.º 1 e n.º 2, do Artigo 10.º da Lei n.º 58/2019), não deve substituir o controlo de acessos à informação de saúde dos cidadãos, que deve ser permitida apenas a quem intervém diretamente nos cuidados de saúde dos utentes e de acordo com a sua função (n.º 7 a), do Artigo 29.º, da Lei n.º 58/2019).

REQUISITOS ADICIONAIS PARA A CERTIFICAÇÃO DO *SOFTWARE* DO RSE

A certificação do *software* do RSE, deverá verificar e validar o cumprimento estrito destes requisitos de segurança e proteção dos direitos dos cidadãos consagrados na legislação vigente, garantindo a existência de mecanismos de controlo de acessos, rastreamento e notificação, entre as quais, dupla autenticação, tais como, palavras-passe robustas, autenticação biométrica (impressão digital ou reconhecimento facial), ou introdução de um código, com identificação do acesso dos profissionais de saúde *role-based,* de forma a permitir o acesso apenas a quem necessita de aceder a essa informação. O titular dos dados deve ser notificado de qualquer acesso realizado aos seus dados pessoais, cabendo ao responsável pelo tratamento assegurar a disponibilização desse mecanismo de rastreabilidade e notificação (n.º 6, do Artigo 29.º, da Lei n.º 58/2019). Na utilização secundária dos dados, para fins de investigação, ou estatísticos, os dados de saúde devem ser anonimizados ou pseudonimizados, com impossibilidade de reidentificação (Artigo 30.º, da Lei n.º 58/2019). A metodologia *OpenEHR*[43] constitui um conjunto de especificações, modelos clínicos e *software*, que incorpora os princípios de interoperabilidade segura de dados abertos, possibilitando a sua utilização secundária em investigação, ao mesmo tempo, que respeita os requisitos do RGPD.

Estes requisitos pressupõem a necessidade de formação de profissionais, quer para o desenvolvimento do *software* do RSE, nomeadamente em soluções abertas, quer para utilizadores e auditores de certificação.

As disposições legais consagradas na legislação vigente que salvaguardam os direitos dos cidadãos relativamente aos seus dados de saúde demonstram o respeito do governo pelos seus cidadãos, pelo que é de crucial importância que seja confirmado o seu cumprimento no desenho e funcionalidades do *software* do RSE, tornando a sua certificação, por entidade de terceira parte independente e imparcial, de extrema importância.

Deve ser possível a segmentação de dados, com possibilidade de encriptação, nomeadamente, dos dados de saúde sensíveis. Informação sensível deve ser sempre encriptada em todas as situações, quer seja para utilização local, armazenamento central ou transmissão.

Em situações inesperadas de emergência ou acidente, em que o acesso à informação de saúde deve ser facilitado, a ISO publicou recentemente uma norma que normaliza um conjunto mínimo de dados clínicos, que permite aos profissionais de saúde disporem da informação essencial e relevante[44].

O RSE atual, da responsabilidade tecnológica da SPMS, E.P.E., é constituído pela Área do Profissional, Área Institucional e Área Pessoal do SNS 24, estando as permissões de acesso aos profissionais de saúde do setor público concedidas por defeito, com possibilidade de alteração pelo cidadão, caso seja pretendido não conceder o acesso.

A interoperabilidade técnica e semântica entre o RSE e os vários sistemas de informação da saúde, fazem-se através de normas internacionais como o HL7 FHIR e a SNOMED CT.

Os dados de saúde existentes no Resumo Clínico Único, do atual RSE, podem eventualmente ser partilhados, mediante consentimento, com um médico registado num dos Estados-Membros da União Europeia, no contexto da prestação de cuidados de saúde e no âmbito da *eHealth Digital Service Infrastructure*.

O PROCESSO DE CERTIFICAÇÃO

A certificação do *software* de RSE deve abranger todas as fases do seu ciclo de vida.

É um processo complexo que exige uma rigorosa avaliação por profissionais experientes, sujeitos às mesmas regras de privacidade e proteção de dados, sendo a certificação profissional dos auditores desejável, sendo mesmo um requisito para a conformidade com algumas normas, nomeadamente a que normaliza os processos de ciclo de vida do *software*[45].

O processo de certificação do *software* de RSE varia entre países, bem como alguns dos critérios de regulamentação, mas basicamente seguem os seguintes passos:

1 - Escolha de um Organismo de Certificação independente de terceira parte, devidamente autorizado e acreditado, para avaliar e certificar o *software* de RSE e que possa garantir por escrito que este cumpre os requisitos das normas e regulamentos.

Em Portugal, o Instituto Português de Acreditação, I.P. (IPAC)[46]. é a autoridade competente para a acreditação dos Organismos de Certificação de Produtos, Processos e Serviços, nomeadamente na matéria de proteção de dados, bem como, para a acreditação de Organismos de Certificação de Pessoas.

2 - Submeter o respetivo *software* do RSE ao processo de avaliação, com a identificação do produto e a apresentação da documentação relevante, nomeadamente, manuais de utilização, descrição das características técnicas e requisitos do *software*, gestão da qualidade e relatórios de testes efetuados. Geralmente começa com uma avaliação do processo de desenvolvimento que inclui codificação, testagem e documentação, seguida de uma revisão detalhada do desenho e das características e capacidades do *software*.

3 - Constatação de um sistema de gestão do risco, inicialmente com identificação e análise dos potenciais riscos, seguida da sua avaliação e respetivo controlo.

4 - Submissão a testagem de verificação: o *software* do RSE tem de se submeter a vários métodos de testagem para assegurar que está em conformidade com as normas relevantes e legislação regulamentar e identificar eventuais vulnerabilidades e potenciais riscos de segurança.

5 - No caso de ser positiva a avaliação pelo Organismo de Certificação, quer nos requisitos, quer nos testes de verificação e validação, será concedida a Certificação e emitido o respetivo Certificado de Conformidade, bem como o direito de uso da Marca de Certificação. É possível, no cumprimento dos requisitos, a obtenção do Selo Digital em Cibersegurança.

6 - Manter a certificação válida, implica a submissão periódica ao mesmo processo de averiguação para a eventual identificação de novas vulnerabilidades e para assegurar que alterações na evolução do *software* se mantêm em conformidade com os requisitos pré-definidos, normas e legislação regulamentar, que são também frequentemente sujeitas a atualizações.

RECOMENDAÇÕES DA CS/09

1- Portugal deverá ter um Registo de Saúde Eletrónico (RSE) único, que abranja todos os setores da saúde, nomeadamente, público, privado, social e militar, com a adequada infraestrutura de suporte, no que diz respeito a *hardware,* acesso à rede e conectividade com a *internet*.

2- O *software* do RSE deverá ser certificado, sendo o processo de certificação desenvolvido de acordo com o modelo a criar e que garanta:
   a) O cumprimento das normas nacionais (NP) e internacionais (ISO/CEN) existentes e a legislação portuguesa vigente;
   b) A normalização e integração dos dados de saúde existentes e a interoperabilidade no desenvolvimento de novos sistemas de informação;
   c) A segurança, confidencialidade e privacidade dos dados individuais de saúde, com encriptação de dados sensíveis e controlo de acessos, permitidos apenas aos profissionais de saúde diretamente relacionados com a assistência ao utente;
   d) Rastreabilidade das alterações à informação introduzida e dos acessos, com notificação ao utente de quem acedeu aos seus dados de saúde;
   e) Existência de um sistema de gestão de risco, que contemple a segurança contra acessos não autorizados, perda acidental de dados e deteção e resposta a vulnerabilidades, incluindo ciberataques;
   f) Utilização fácil e intuitiva, baseada na opinião fundamentada dos utilizadores;
   g) Viabilização da escalabilidade e estrutura dinâmica do RSE;
   h) Inclusão de novas dimensões do RSE ainda não contempladas;
   i) Possibilidade da partilha transfronteiriça dos dados de saúde, com consentimento explícito do titular dos dados;
   j) Capacidade de reutilização dos dados e repositórios de dados abertos e anonimizados para investigação e desenvolvimento.

3- Criação da figura do auditor de sistemas de informação para a saúde.

CONCLUSÃO

Na sequência dos desafios, exigências e ameaças, e da evolução das tecnologias de informação que têm surgido ao longo dos anos, este texto, não sendo exaustivo, procurou sintetizar a situação atual e apontar recomendações para a existência de um Registo de Saúde Eletrónico, que efetivamente cumpra a legislação, que existe, mas que não é suficiente, se não houver forma de assegurar que é de facto cumprida.

A Certificação e Recertificação do *software* do Registo de Saúde Eletrónico é uma garantia do cumprimento contínuo dos critérios da qualidade e dos direitos dos cidadãos, relativamente à segurança e privacidade dos seus dados de saúde, cabendo ao governo tomar essa opção, definindo e tomando as medidas adequadas para que sejam cumpridas as respetivas normas e a legislação.

REFERÊNCIAS BIBLIOGRÁFICAS

1- Weed LL. Medical records, patient care, and medical education. Ir J Med Sci 1964 Jun;39(6): 271-82 http://doi.org/10.1007/BF02945791
2- McDonald CJ, Overhage JM, Tierney WM, et al. The Regenstrief Medical Record System: a quarter century experience. Int J Med Inform. 1999 Jun;54(3):225-53. http://doi: 10.1016/s1386-5056(99)00009-x.
3- Neves AL, et al. Impact of providing patients access to electronic health records on quality and safety of care: a systematic review and meta-analysis. BMJ Qual Saf 2020;29:1019 –1032. http://doi:10.1136/bmjqs-2019-010581
4- Health Insurance Portability and Accountability Act of 1996 (HIPAA): US Department of Health and Human Services: https://www.hhs.gov/hipaa/for-professionals/index.html
5- Evans RS. Electronic Health Records: Then, Now, and in the Future. Yearb Med Inform 2016 Suppl1:S48-61 http://dx.doi.org/10.15265/IYS-2016-s006
6- Serviços Partilhados do Ministério da Saúde, E.P.E.: https://www.spms.min-saude.pt
7- Decreto-Lei n.º 61/2022, de 23 de setembro. Diário da República n.º 185/2022, Série I de 2022-09-23
8- European Institute for Health Records (EuroRec), https://www.eurorec.org
9- European Commission. eHealth Digital Service Infrastructure (eHDSI): Electronic cross-border health services: https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en
10-Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022: L_2022323PT.01000401.xml - EUR-Lex
11-Blumenthal D, Tavenner M. The "meaningful use" regulation for electronic health records. N Engl J Med 2010 Aug;363(6):501-4 http://doi: 10.1056/NEJMp1006114
12-Portela D, Frade S, Patrício P, Cruz-Correia R. Perspetivas sobre o Presente e Futuro dos Registos Eletrónicos de Saúde em Portugal. Acta Med Port 2022 Oct;35(10):713-717 http://doi.org/10.20344/amp.17857
13-Virginio L, Ricarte I. Identification of Patient Safety Risks Associated with Electronic Health Records : A Software Quality Perspective. Studies in Health Technology 2015 Aug; 216:55-9
14-Regulamento (UE) N.° 1025/2012 do Parlamento Europeu e do Conselho de 25 de outubro de 2012 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012R1025
15-ISO/IEC 25010 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Systems and software quality models
16-ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements
17-ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls
18-NP ISO 31000:2018 – Gestão do risco – Linhas de orientação
19-ISO 10781:2023, Health informatics – HL7 Electronic Health Record-System Functional Model, Release 2.1 (EHR FM)
20-Vorisek CN, Lehne M, Klopfenstein SAI, Mayer PJ, Bartschke A, Haese T, Thun S. Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review. JMIR Med Inform. 2022 Jul;10(7):e35724 http//doi: 10.2196/35724: 10.2196/35724
21-ISO 13972, Health informatics – Clinical information models – Characteristics, structures and requirements
22-ISO/TS 18864, Health informatics – Quality metrics for detailed clinical models

23-SNOMED CT : https://www.snomed.org
24-Manukyan E, Levine B, Manukyan A, Lulejian A. Integration of Laboratory Data into a National Electronic Health Record (EHR). Stud Health Technol Inform. 2023 Jun 29:305:491-494 http://doi: 0.3233/SHTI230540
25-ISO 12052, Health informatics – Digital imaging and communication in medicine (DICOM) including workflow and data management.
26-ISO/IEC 82304, Health software – Part 1: General requirements for product safety
27-NP ISO 18308:2017 Informática em saúde - Requisitos para uma arquitetura de registo eletrónico de saúde - (ISO 18308:2011)
28-ISO 13606:2019, Health informatics – Electronic health record communication. Part 1: Reference model
29-ISO 13606-2:2019, Health informatics – Electronic health record communication. Part 2: Archetype interchange specification
30-ISO 13606-3:2019, Health informatics – Electronic health record communication. Part 3: Reference archetypes and term lists
31-ISO 13606-4:2019, Health informatics – Electronic health record communication. Part 4: Security
32-ISO 13606-5:2019, Health informatics – Electronic health record communication. Part 5: Interface specification
33-ISO 12967, Health informatics – Service archictecture (HISA)
34-ISO 27799, Health informatics – information security management in health using ISO/IEC 27002
35-ISO 27789:2021, Health informatics – Audit trails for electronic health records
36-Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881
37-Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021R0694
38-Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679
39-Lei n.º 58/2019, de 8 de agosto. Diário da República n.º 151/2019, Série I de 2019-08-08,
40-Lei n.º 59/2019, de 8 de agosto. Diário da República n.º 88/2019, Série I de 2019-05-08
41-Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016
42-ISO/TS 17975:2022, Health informatics – Principles and data requirements for consent in the collection, use or disclosure of personal health information
43-OpenEHR Foundation: www.openehr.org
44-ISO 27269:2021 (en) Health Informatics – The International Patient Summary
45-ISO/IEC 12207 Systems and software engineering- Software life cycle processes
46-Instituto Português de Acreditação http://www.ipac.pt