Propostas de Melhoria da Segurança dos Sistemas de Informação Clínica em Portugal

Sara Araújo, João Pascoal Faria, José Magalhães Cruz

Faculdade de Engenharia da Universidade do Porto, Portugal
Rua Dr. Roberto Frias, 4200-465 Porto
mrs01012@fe.up.pt; jpf@fe.up.pt; jmcruz@fe.up.pt

Resumo

Com vista à melhoria dos cuidados de saúde prestados ao cidadão, assiste-se ao crescente registo e circulação de informação clínica em formato electrónico. Este facto traz consigo preocupações acrescidas com a segurança e privacidade dessa informação. Da análise da situação actual nos sistemas de informação clínica do Serviço Nacional de Saúde (SNS) em Portugal, ressaltam um conjunto de fragilidades, que podem ser minoradas se as propostas de melhoria da segurança, aqui apresentadas, for acolhido. Defende-se, nomeadamente, a implementação de uma infra-estrutura de chaves públicas (PKI) e a definição de uma política de segurança concertada ao nível das instituições ligadas ao SNS, em conformidade com as normais internacionais existentes.

Palavras-chave: Segurança, Sistemas de Informação Clínica, Normas, Infra-estrutura de Chaves Públicas (PKI - Public Key Infrastructure)

Introdução

O registo electrónico dos dados clínicos dos pacientes e a sua partilha entre todos os profissionais envolvidos é fundamental para a optimização dos processos de prestação de cuidados de saúde. Para que o registo e circulação da informação clínica em formato electrónico seja bem aceite, deve ser assegurada a sua fiabilidade e protecção. É importante conseguir um bom compromisso entre dois objectivos que por vezes entram em conflito: melhorar os cuidados de saúde prestados ao cidadão e garantir a privacidade, integridade e disponibilidade dos seus dados clínicos. Isso pode ser conseguido com sistemas de informação clínica **seguros**.

Requisitos de Segurança dos Sistemas de Informação Clínica

Um sistema de informação clínica compreende aplicações informáticas, equipamentos informáticos (computadores, redes) e bases de dados que são utilizados pelos profissionais de saúde (médicos, enfermeiros, administrativos, etc.) para registar, manipular e consultar dados em diferentes formatos (texto, imagem, etc.). Estes dados, sobre a saúde e a doença dos pacientes (história clínica, diagnósticos, tratamentos,

prescrições, consultas, etc.), são indispensáveis à prestação de cuidados de saúde mas também servem à investigação clínica, à formação médica e à gestão desses cuidados.

Em qualquer um dos elementos do sistema de informação clínica existem vulnerabilidades que podem ser exploradas.

Características de Segurança a considerar

Atendendo à importância e sensibilidade da informação manipulada, os sistemas de informação clínica devem garantir um conjunto de características de segurança:

Confidencialidade: é necessário garantir que os dados dos pacientes são protegidos, não podendo ser acedidos por pessoas não autorizadas, seja de forma acidental ou deliberada. A confidencialidade pode ser posta em risco por razões técnicas ou organizacionais: mecanismos de controlo de acesso insuficientes, transmissão de informação não cifrada pela rede, partilha de senhas entre utilizadores, definição desadequada de privilégios dos utilizadores, falta de cuidado no manuseio da informação, etc.

Disponibilidade: é necessário garantir que os recursos e serviços chave dos sistemas de informação clínica estão acessíveis quando forem necessários, particularmente em situações de emergência ou em cuidados intensivos. Os recursos e serviços podem ficar indisponíveis por avarias nos equipamentos ou no ambiente onde operam (por exemplo, quebras de energia, falhas nas aplicações, erros no manuseamento do sistema, ataques intencionais, causas naturais como incêndios ou inundações), insuficiência de recursos, etc. Para evitar quebras de disponibilidade, é necessário existirem mecanismos de redundância, recuperação de falhas e protecção contra ataques, entre outros.

Integridade: é necessário garantir que a informação clínica armazenada ou em trânsito não é corrompida ou alterada indevidamente, de forma deliberada ou acidental, devido a erros operacionais (na introdução e manipulação de dados), erros no *software*, vírus, mau funcionamento do equipamento, etc. Uma das medidas que pode ser tomada para proteger a informação contra ataques à integridade é a utilização de selos digitais.

Em situações de transacção de informação clínica, é ainda importante garantir que as entidades intervenientes são quem afirmam ser (**autenticidade**), e que não podem negar posteriormente a sua participação na transacção (**não repúdio**).

A Situação Actual

O nível de informatização do SNS tem vindo a aumentar nos últimos anos. A Rede Informática da Saúde (RIS) interliga as principais instituições do SNS e estão amplamente disseminadas aplicações clinico-administrativas desenvolvidas pelo Instituto de Gestão Informática e Financeira da Saúde (IGIF) [1], de que se destacam o SONHO, SINUS e SAM/SAPE (ver Figura 1).

Esta informatização acelerada traz como consequências

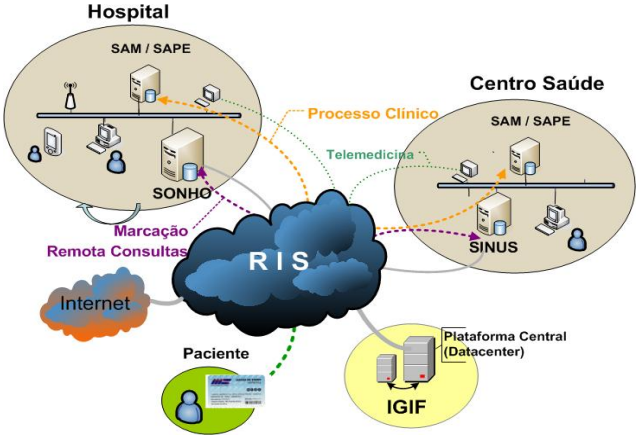

Figura 1 – Sistema de Informação Clínica no SNS

uma maior exposição da informação sensível a um ambiente de sociedade de informação, basicamente hostil.

A análise da situação actual dos sistemas de informação clínica em Portugal, mostra que não estão definidas políticas e mecanismos de segurança adequados e ao nível de todo o SNS. Outros problemas identificados que podem ameaçar a segurança dos sistemas de informação clínica têm a ver com as tecnologias obsoletas em uso, a não integração dos sistemas e o comportamento descuidado dos utilizadores. Exemplo desta situação é o facto de algumas das aplicações mais importantes (SONHO/SINUS) ainda se basearem em interacções de terminal desprotegidas; outro exemplo, é a negligência na movimentação e, até, partilha de senhas de acesso e no abandono temporário de postos de trabalho com sessões abertas.

Propostas para a Melhoria da Segurança dos Sistemas de Informação Clínica

Dada a situação exposta, que revela as fragilidades de segurança do sistema informático de saúde, afigura-se imperativo melhorar a protecção da informação clínica. É importante utilizar políticas e mecanismos de segurança que tenham uma abrangência global, não podendo ser confinadas a unidades de saúde isoladas. Assim, apresentam-se sugestões de algumas soluções de melhoria que vão no sentido de implementar no SNS: um plano de segurança global; uma infra-estrutura de chaves públicas; melhores meios de identificação profissional.

Definição de um Plano de Segurança Global

Tal plano deverá abranger todas as unidades de saúde que integram a RIS e outras entidades privadas com a qual exista articulação (hospitais, clínicas, laboratórios, farmácias, etc.). Deverá centrar-se em políticas de segurança globais que forneçam orientações para reduzir riscos e garantir a integridade, confidencialidade e disponibilidade da informação clínica. Isso conduziria à utilização de métodos de validação e correcção de dados, de codificação e parametrização da informação e à realização de auditorias periódicas.

Uso de melhores mecanismos de protecção

O alargamento do uso de mecanismos de autenticação forte, por exemplo utilizando técnicas biométricas, deveria ser incentivado. Tal opção, associada ao uso de um *smart card* como cartão de identificação profissional permitiria ainda o aumento significativo do nível de controlo de acessos: tal cartão seria intransmissível e o seu cancelamento poderia ser feito de imediato; quando o utilizador abandonasse o posto de trabalho, obrigatoriamente teria de se fazer acompanhar do respectivo cartão, pelo que o *logout* seria automático e inevitável. No caso de tal cartão incluir também tecnologia RFID (Radio Frequency Identification), a sua utilização seria extremamente cómoda, pois o profissional de saúde não teria sequer necessidade de o retirar do seu local de fixação.

Ao nível da infra-estrutura, o uso de *firewalls*, sistemas criptográficos fortes e medidas organizacionais (tais como a gestão de permissões, de regras de acesso, de

perfis de utilizador e contínua formação dos utilizadores) permitiria aumentar a confiança na segurança do sistema. Para garantir a disponibilidade da informação clínica, do equipamento ou serviços de rede recomenda-se ainda a melhoria da implementação de mecanismos de redundância (duplicação de equipamento central), a realização cuidada de cópias de segurança e o aumento das inspecções periódicas (das instalações físicas, informáticas, eléctricas, etc.).

Utilização de uma infra-estrutura de chaves públicas

Propõe-se a utilização de uma infra-estrutura de chaves públicas hierárquica em que a entidade de topo seria a recém criada "Entidade Certificadora Electrónica do Estado" [2], a entidade certificadora associada para a área da saúde seria o IGIF e as instituições de forma individual ou agrupada seriam responsáveis pela gestão de todo o ciclo de certificação nas suas instituições. Sugere-se o IGIF como autoridade certificadora para a área da Saúde porque, para além de ter um papel normalizador, já é a entidade responsável pela gestão da RIS e de grande parte das aplicações instaladas nas unidades de saúde e possui os meios para actuar ao nível desta infra-estrutura.

A infra-estrutura proposta baseia-se no uso de sistemas criptográficos assimétricos, ditos de "chave pública". Nestes sistemas, é atribuído a cada utilizador um par de chaves: uma chave a publicitar (pública) e uma chave a esconder (privada). A chave pública seria disponibilizada livremente em certificados digitais ou num directório de acesso público (por exemplo, na página *web* da instituição) e a chave privada deveria ser guardada em local de confiança do utilizador (por exemplo, no seu cartão de identificação profissional). Cada certificado seria assinado digitalmente pela autoridade certificadora escolhida,que é o vértice superior do triângulo de confiança necessário para o estabelecimento de sessões seguras na rede entre as partes associadas aos vértices da base do triângulo (ver Figura 2).

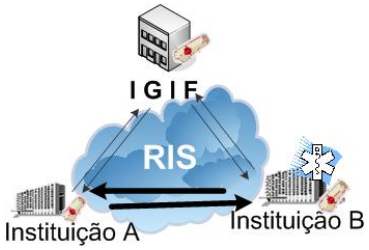

Figura 2 – Triângulo de Confiança

Tal autoridade representa um papel muito importante em termos da segurança da informação que transita na rede, pois possibilita a criação de uma relação de confiança entre parceiros intervenientes nos cuidados de saúde dados aos pacientes.

Conformidade com Normas Internacionais

A necessidade de frequente trocas de informação clínica e a garantia de serem efectuadas com segurança exige uma grande interoperabilidade entre os sistemas informáticos de todas as instituições envolvidas. Para se conseguir isso, há que exigir conformidade com normas do sector de saúde aceites internacionalmente. HL7 [3], DICOM [4], HIPAA [5], CEN/TC 251 (WGIII) - Security, Safety and Quality [6], ISO TC 215 (WG 4) - Security [7], são exemplos significativos dessas normas.
Isto permitiria, sem por em risco a protecção da informação clínica, a sincronização de informação entre fontes diferentes (em termos de *software*, equipamento e instituições).

Conclusão

Uma rede de comunicações eficiente e eficaz é vital para a partilha e o acesso à informação clínica que frequentemente se encontra em servidores de bases de dados localizados remotamente. O grande volume de dados clínicos do SNS tem que ser suportado por boas infra-estruturas de comunicações, tecnologias e programas informáticos, para que em qualquer situação se possa ter um bom e correcto desempenho. Ao mesmo tempo, há que exibir uma troca e armazenamento seguro da informação, de acordo com as necessidades dos sistemas de informação clínica.

As propostas apresentadas têm por finalidade estabelecer orientações genéricas a adoptar pelas instituições e que deverão ser embebidas noutros processos específicos às instituições, com o principal objectivo de colmatar as principais vulnerabilidades identificadas na gestão e utilização da informação clínica.

A segurança da informação é uma questão dinâmica, o ritmo das mudanças tecnológicas gera continuamente novos desafios para a politica de segurança global, pelo que o esforço com a segurança deve ser contínuo.

Há que bem proteger a privacidade do paciente e este tem de confiar na instituição onde é tratado e onde confia a guarda dos seus dados pessoais.

Referências

[1] http://www.igif.min-saude.pt, Instituto de Informática Gestão Financeira da Sáude, Ab 2007

[2]http://www.portugal.gov.pt/Portal/PT/Governos/Governos_Constitucionais/GC17/Ministerios/PCM/MP/Comunicacao/Outros_Documentos/20051006_MP_Doc_ECEE.htm, Entidade Certificadora Electrónica do Estado, Ab 2007

[3] http://www.nema.org, especificações da norma DICOM, Ab 2007

[4] http://www.hl7.org, especificações da norma HL7, Ab 2007

[5] http://www.centc251.org, normas do grupo de trabalho nº 251 do CEN, Ab 2007

[6] http://www.iso.org, normas públicadas pelo grupo de trabalho nº 215 da ISO, Ab 2007

[7] http://www.hipaa.org, Health Insurance Portability Accountability Act of 1996, Ab 2007