Confidencialidade, segurança e integridade das informações médicas em rede: Seu impactos na gestão de TI

Renato M.E. Sabbatini

Diretor de Educação e Capacitação Profissional da Sociedade Brasileira de Informática em Saúde, e Presidente do Centro Internacional de Tecnologias de Informação e Comunicação em Saúde, Instituto Edumed para Educação em Medicina e Saúde, Campinas, SP. Contato: sabbatini@edumed.org.br

Resumo

As decisões recentes do Conselho Federal de Medicina sobre a obrigatoriedade das organizações clínicas obedecerem a diversos requisitos de segurança, confidencialidade e integridade das informações clínicas e individuais sobre os pacientes armazenados em sistemas eletrônicos, colocarem subitamente a necessidade de conformidade para dezenas de milhares de softwares, sistemas e entidades em todo o país. Os requisitos, classificados em dois níveis, o NGS1 e NGS2 (Nível de Garantia de Segurança) partem de um nível elementar de segurança (como o uso de login e senha robustos), até chegarem ao uso da certificação digital para proteção, criptografia e assinatura válida de documentos eletrônicos, segundo as normas da Infraestrutura de Chaves Públicas Brasileiras (ICP Brasil). Neste artigo são examinadas as implicações e consequências dessa tendência para áreas como certificação de software médico, impactos sobre sistemas próprios ou adquiridos de terceiros, mudanças na governança e gestão de TI nas organizações clínicas brasileiras, novos produtos e serviços, como telemedicina, e vários outros.

Introdução e Contexto Histórico

Desde o juramento de Hipócrates, grego que é considerado o pai da medicina, e que estabeleceu as bases éticas da prática médica que perduram até hoje, a obrigatoriedade de manter segredo sobre as informações sobre o paciente definiram o que é a confidencialidade e seus limites.

Em tempos modernos, devido à grande importância legal e médica de se preservar essas informações inalteradas e com segurança por um longo período de tempo, o código de ética médico modificou-se para definir também alguns parâmetros de preservação, uso e acesso do que chamamos prontuário de saúde do paciente, registro médico, e outras denominações.

Assim sendo, os registros de saúde, em qualquer formato ou meio, compartilham requisitos de garantia de segurança (RGS) similares a de outros documentos, tais como os das áreas jurídica, cartorial e outras, mas possuem certas características que a especializam e que obrigaram o surgimento de leis, procedimentos e até de profissionais dedicados a essa área.

Até a o final do século XX essas precauções não eram muito necessárias, pois os registros médicos existiam praticamente apenas como documentos em posse dos médicos, na forma de livros ou agendas de anotação, mantidas em folhas encadernadas, ordenadas por data de primeiro contato. Os famosos irmãos Mayo inovaram em seu hospital em Rochester, NY, ao criarem os primeiros prontuários centralizados, um para cada paciente, e que coletavam todos os documentos clínicos, como registros de internações, cirurgias, prescrições, resultados de exames, etc. Desde essa época, então,os registros de saúde em papel foram se aperfeiçoando quanto à organização, guarda e acesso, e constituem até hoje o esteio principal da informação clínica na grande maioria de todas as

organizações clínicas, inclusive os consultórios médicos.

Com o advento da automatização do prontuário médico, surgiram novos problemas e necessidades, porém foi com a implementação universal as redes de computadores é que os perigos de uso indevido, alterações, etc., tornaram-se agudos, Como esse é um fenômeno recente (no Brasil o uso generalizado de redes locais, redes de área ampla e internet tem pouco mais do que uma década de experiência real), ainda estamos em evolução nesses dois aspectos. Países mais avançados do que o nosso em informática na saúde também tem buscado soluções há relativamente pouco tempo. Nos EUA, por exemplo, está em vigor há cerca de 6 anos o HIPAA: Health Information Protection Act, uma legislação que estipula regras rígidas para a preservação da confidencialidade e da segurança da informação em saúde, e que prevê penalidades severas para os casos de violação.

A evolução técnica dos sistemas de segurança e de proteção do acesso eletrônico a documentos digitais, assim como a autenticação de usuários, tem repercutido bastante na área da saúde, impulsionados pela natureza vital e consequências legais sérias. A criptografia, a autenticação segura e inambígua dos usuários, e a assinatura e certificação digitais foram os desenvolvimentos de maior relevância, nesse sentido

Segurança e Proteção da Informação em Saúde no Brasil

Tradicionalmente, por ser o guardião da deontologia médica (código de ética médica), o Conselho Federal de Medicina é a autoridade com prerrogativas de legislar acessoriamente sobre a guarda, uso, acesso e proteção dos dados médicos, principalmente da confidencialidade do paciente. O CFM vem se posicionando desde 2001 quanto às novas tecnologias digitais e seus impactos sobre a informação médica, principalmente porque se preocupou em estabelecer uma Câmara Técnica especializada em novas tecnologias, como informática, telemedicina, prontuário eletrônico, etc. O CFM estabeleceu um convênio com a Sociedade Brasileira de Informática em Saúde em 2003, com o intuito de desenvolver um trabalho mais focado e intenso sobre o problema da proteção da confidencialidade e da regulamentação do uso de sistemas de registro eletrônico de saúde (SRES).

Esse trabalho conjunto do CFM e da SBIS teve dois resultados importantes;

1. Uma resolução normativa (no 1821, de 2007), que definiu alguns pontos importantes e regulamentou o uso de SRES, principalmente no que diz respeito aos quesitos de segurança e proteção da confidencialidade, e já prevendo que o CFM seria a autoridade certificadora (AC) para os certificados digitais dos médicos brasileiros; e
2. Um conjunto de normas e requisitos pela SBIS, de certificação de software para SRES, com base na resolução acima citada.

A Resolução CFM 1821 foi um marco extremamente importante para a história do desenvolvimento do processo de certificação de SRES no Brasil, e de certa forma representou uma iniciativa pioneira em nível mundial. O objetivo da resolução foi "aprova(r) as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde."

O caminho da certificação foi definido como o mais adequado para o contexto brasileiro, principalmente porque já tinham surgido em nível internacional vários padrões para tal. Mais importante, ainda, a Resolução abriu o caminho, pelo menos quanto ao uso dos SRES por médicos, para um objetivo longamente desejado, que é o da eliminação do papel e das assinaturas físicas e carimbos de identificação que até então eram estritamente obrigatórias para qualquer documento

médico identificado.

Foi constituída na SBIS, então, uma gerência específica para o processo de certificação. O grupo de trabalho de certificação, que contou em sua composição com vários especialistas da Sociedade, e alguns consultores contratados, definiram que o estabelecimento da certificação seguiria duas etapas, com a finalidade de ganhar experiência e permitir que as empresas e instituições que desejassem, pudessem já adaptar seus sistemas às normas já definidas pelo CFM.

1. A primeira fase era de auto-conformidade, ou seja, a SBIS produziu um Manual de Requisitos para SRES. As empresas e instituições dispunham de um check-list de verificação de requisitos, e se conseguisse alcança-los, declarava sua conformidade aos mesmos, passando a integrar uma lista publicada pela SBIS. Nesta fase não havia nenhum tipo de auditoria ou inspecção por parte de profissionais independentes
2. Na segunda fase, no entanto, previu-se a realização de uma auditoria especializada, feita por profissionais auditores treinados pela SBIS e vinculados à sua Gerência de Certificação. O processo de certificação foi definido em um novo Manual (na versão 3.3, atualmente) e implementava normas de estrutura e conteúdo, bem como garantia de dois níveis de segurança (NGS), sendo que o NGS2 implica, em conformidade com as decisões do CFM, em uso de certificação digital de acordo com a Infraestrutura de Chaves Públicas do Brasil (ICP) e o uso de assinatura digital. O processo detalhado de auditoria foi também definido em um Manual de Ensaios e Análises (atualmente em sua versão 1.2), e que basicamente consiste na execução e observação do SRES com relação a cerca de 152 requisitos obrigatórios, através da simulação de cenários típicos de uso em uma instituição de saúde.

A Fase I obteve sucesso, com o registro voluntário de cerca de 32 sistemas. Para a capacitação de auditores e usuários para a fase II, foi desenvolvido pela Gerência de Certificação da SBIS um curso presencial, que foi realizado até o momento oito vezes, e que formou mais de 300 pessoas. Atualmente está sendo montado um curso similar, na modalidade a distância, em cooperação como a Diretoria de Educação e Capacitação Profissional da SBIS. Um segundo curso, de capacitação prática e de credenciamento de auditores está sendo preparado, e contará com um treinamento baseado em um simulador próprio de RES. Até junho de 2010, tinham sido certificados de acordo com os requisitos da fase II, quatro sistemas. A listagem dos mesmos podem ser encontrados no site de certificação da SBIS.

Uma questão ainda em progresso é a referente aos subsistemas que podem ser certificados. Até o momento (junho de 2010), a SBIS certificava apenas sistemas de atenção ambulatorial (requisitos de estrutura e funcionalidades. NGS1 e NGS2), TISS (o documento padronizado adotado no Brasil para o faturamento médicc hospitalização. Outros subsistemas importantes, com PACS (Picture Archiving and Communication Systems(, RIS (sistemas de informação radiológica), LIS (sistemas de informação de laboratórios), GED (sistema de gerenciamento de documentos em armazenamento óptico), sistemas de internação hospitalar, e vários outros, ainda não foram especificados pela SBIS quantos aos seus requisitos.

Implicações para a Gestão de TI nas Organizações Clínicas

Existem alguns pontos importantes da Resolução CFM 1821/2007 que devem ser examinados quanto ao seu impacto na gestão de TI das organizações clínicas:

1. Os documentos digitalizados ou gerados eletrônicamente e que forem assinados digitalmente pelos profissionais responsáveis identificados, segundo as normas do NGS2, dispensam a cópia em papel;

2. A guarda de documentos em papel não registrados em um sistema de gestão eletrônica de documentos certificada pelo NGS2 é de 20 anos;
3. Os documentos digitalizados, bem como os documentos gerados eletrônicamente, não tem data determinada obrigatória de guarda, isto é, devem ser preservados digitalmente por tempo indefinido;
4. Os documentos eletrônicos devem ser cópia fiel e conter todas as informações de seus equivalentes em papel; e
5. A partir do momento em que o CFM implementar a identidade digital (e-CRM), como entidade certificadora, o seu uso será obrigatório por todos os médicos, e as instituições terão o prazo de um ano para implementarem o NGS2, obrigatoriamente.

Tomados isoladamente ou em conjunto, essas normas criam uma série de problemas novos para os gestores de TI e desenvolvedores, bem como impactos significativos nos custos operacionais de TI nas organizações de saúde:

1. Necessidade de instalar redes de computadores, e terminais de captura e consulta de dados em todos os pontos de um hospital, ambulatório, clinica, consultório, unidade básica de saúde, etc.,ou seja, em qualquer local onde sejam atendidos pacientes. Esses terminais terão que ser compatíveis com a leitura e operação, com respectivos drives, de certificados digitais (smartcards ou tokens baseados no padrão USB);
2. Os servidores usados pela instituição deverão ser expandidos;
3. Necessidade de adquirir ou desenvolver SRES ambulatoriais (por enquanto) e de internação (no futuro), totalmente integrados, e em conformidade com os requisitos de NGS2;
4. Obrigatoriedade de emitir certificados digitais para todos os profissionais clínicos (e não apenas para médicos) que tenham autorização para utualizar os SRES, e o pagamento da renovação dos mesmos a cada 3 anos, de acordo com o ICP Brasil;
5. O estabelecimento efetivo e operação de uma Comissão Permanente de Avaliação de Documentos (CPAD), e de um sistema de gestão eletrônica de documentos (GED);
6. Treinamento ou retreinamento de todos os funcionários, médicos, enfermeiros, técnicos, etc., envolvidos com o SRES.
7. Sistemas de telemedicina e sistemas portáveis (em smartphones e PDAs, por exemplo) deverão obedecer ao NGS2 também;
8. Sistemas RES que importam ou exportam dados para outros sistemas deverão obedecer aos requisitos NGS1 ou NGS2, se for o caso
9. A emissão de documentos em papel, quando ocorrer, deverá ser identificada com a assinatura digital e permanecer registrada no sistema;
10. Os registros de transações (logs) e trilhas de auditoria dos SRES deverão ser identificados digitalmente
11. O tráfego de dados entre servidores distintos deverá ser protegido por criptografia, assim como os bancos de dados. O item anterior e este terão impactos significativos sobre o desempenho dos sistemas, exigindo investimentos em hardware e software com maior desempenho e maior capacidade de armazenamento de dados.

Como se pode depreender pela breve lista acima, os impactos principais na gerão de TI serão principalmente no aumentos dos custos de aquisição e operacionais, inclusive vários custos recorrentes, como a manutenção dos certificados digitais, a adaptação ou redesenvolvimento de software, e o estabelecimento de novas rotinas administrativas e de fluxos de dados, de novas organizações, e de treinamento dos usuários.

Por outro lado, o aumento da segurança e da proteção de confidencialidade usando certificados e assinaturas digitais traz benefícios inegáveis, como a simplificação de vários processos de autenticação, e, principalmente, da dispensa do uso de papel, e de armazenamento de recursos

físicos. Embora o NGS2 ainda não seja obrigatório, não há dúvidas que o será algum dia. Portanto, as empresas desenvolvedoras de software para SRES, bem como as instituições que usam sistemas de desenvolvimento próprio, terão que investir na adaptação, redesenvolvimento, e auditoria de certificação de seus SRES.

Como a auditoria da SBIS é cara e complexa, pagando-se por módulos e necessitando-se pagar adicionais caso na primeira auditoria não tenha se atingido conformidade em todos os requisitos obrigatórios, recomendamos que seja contratada uma consultoria chamada de pré-certificação, que irá auxiliar a empresa a rever um a um todos os requisitos estruturais, funcionais e de segurança, realizar simulações da auditoria e recomendar soluções para as inconformidades observadas. É um investimento que vale a pena ser feito, como uma prevenção, mas também como um processo de melhoria da qualidade do software e dos processos.

Referências

1. Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) versão 3.3 (edição 2009)
2. Manual Operacional de Ensaios e Análises para Certificação de S-RES versão 1.2 (edição 2009
3. Resolução CFM No.1821/2007