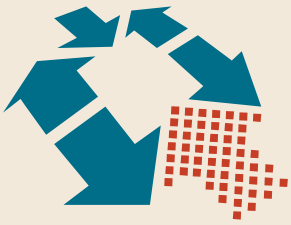

PADRÃO **TISS**

segurança & **privacidade**

novembro 2013

ANS Agência Nacional de Saúde Suplementar

O componente de segurança e privacidade do Padrão TISS, contou com a Sociedade Brasileira de Informática em Saúde – SBIS como entidade de referência e estabelece os seguintes requisitos:

Descrição	Condição de utilização
1. Identificar e autenticar todo usuário antes de qualquer acesso a dados com identificação do beneficiário.	Obrigatório
2. Utilizar para autenticação de usuários a site e páginas da Internet (portais) login e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital.	Obrigatório
3. Utilizar para autenticação de usuários, via utilização de webservices, login e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital em substituição ao login e senha.	Obrigatório
4. Verificar a qualidade de segurança da senha no momento de sua definição pelo usuário obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser não alfabético	Obrigatório
5. Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento.	Obrigatório

Descrição	Condição de utilização
6. Armazenar a senha dos usuários utilizando qualquer algoritmo HASH.	Obrigatório
7. Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de login. Este número de tentativas não deve ser superior a cinco.	Obrigatório
8. Possuir controles de segurança na sessão de comunicação a fim de não permitir o roubo de sessão do usuário	Obrigatório
9. Oferecer os seguintes serviços de segurança na sessão de comunicação entre o componente cliente e o componente servidor: autenticação do servidor, integridade dos dados e confidencialidade dos dados.	Obrigatório
10. Encerrar a sessão do usuário após período de tempo configurável de inatividade. Este tempo não deve ser superior a trinta minutos.	Obrigatório
11. Registrar log de acessos e de tentativas de acesso ao sistema de informação.	Obrigatório
12. Utilizar certificado digital sempre dentro do período de validade além de não aceitar o certificado se o mesmo estiver na lista de certificados revogados da AC.	Obrigatório
13. Utilizar certificado digital que identifique o endereço eletrônico	Obrigatório

Descrição	Condição de utilização
para o qual foi emitido	
14. Utilizar certificado digital que contemple em sua estrutura a identificação da autoridade certificadora emissora.	Obrigatório
15. Utilizar certificado digital que contemple em sua estrutura a identificação do titular do certificado	Obrigatório
16. Utilizar certificado digital que utilize protocolo criptográfico SSL ou TLS	Obrigatório
17. Utilizar certificado digital que utilize criptografia de, no mínimo, 128 bits	Obrigatório
18. Utilizar certificado digital que implemente autenticação por algoritmo HASH	Obrigatório
19. A interrupção do serviço de troca eletrônica de informações entre prestadores de serviços de saúde e operadoras de planos privados de assistência à saúde deve ser solucionada em até 48 (quarenta e oito) horas, salvo em caso fortuito ou de força maior devidamente justificado.	Obrigatório
20. Para as transmissões remotas de dados identificados, os sistemas das operadoras de planos de saúde deverão possuir um certificado digital de aplicação única emitido por uma Autoridade Certificadora.	Obrigatório

Descrição	Condição de utilização
21. As operadoras de planos privados de assistência à saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial à toda informação identificada individualmente.	Obrigatório
22. Deve conter a assinatura digital do prestador de serviços na guia de cobrança de internações para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional
23. Deve conter a assinatura digital do prestador de serviços na guia de cobrança de SP/SADT para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional
24. Deve conter a assinatura digital do prestador de serviços na guia de cobrança de consultas para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional
25. Deve conter a assinatura digital do prestador de serviços na guia de cobrança de serviços de odontologia para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional
26. Os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial a toda informação identificada individualmente.	Recomendado
27. Seguir os itens de segurança descritos na *Cartilha Sobre Prontuário Eletrônico para sistemas de registro eletrônico de*	Recomendado

Descrição	Condição de utilização
saúde construída através de convênio, entre o CFM e a SBIS.	
28. Observar a Resolução CFO-91/2009 que aprova as normas técnicas concernentes à digitalização, uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, quanto aos Requisitos de Segurança em Documentos Eletrônicos em Saúde.	Recomendado
29. Observar a RESOLUÇÃO CFM Nº 1.821/07 que aprova 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.	Recomendado
30. Deve conter a assinatura digital do prestador de serviços na mensagem enviada a operadora para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional
31. Deve conter a assinatura digital da operadora na mensagem enviada ao prestador de serviços para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional

ANS Agência Nacional de Saúde Suplementar

Ministério da Saúde

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Av. Augusto Severo, 84 - Glória
Rio de Janeiro-RJ 20021-040

www.ans.gov.br
Disque-ANS: 0800 701-9656