



Manual de Certificação para Sistemas de Registro Eletrônico em Saúde

Versão 3.0

Editores:

**Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa
John Lemos Forman**

Novembro de 2007

Conselho Federal de Medicina Diretoria

Gestão de: 13/10/2004 à 12/10/2009

Presidente:	Edson de Oliveira Andrade
1º Vice-Presidente:	Roberto Luiz D'Avila
2º Vice-Presidente:	Rafael Dias Marques Nogueira
3º Vice-Presidente:	Gerson Zafalon Martins
Secretário-geral:	Livia Barros Garcao
1º Secretário:	Henrique Batista e Silva
2º Secretário:	Clóvis Francisco Constantino
Tesoureiro:	José Hiran da Silva Gallo
2º Tesoureiro:	Ricardo José Baptista
Corregedor:	Pedro Pablo Magalhães Chacel
Vice-Corregedor:	Jose Fernando Maia Vinagre

Câmara Técnica de Informática em Saúde e Telemedicina

Roberto Luiz D'Avila (Coordenador)
Cláudio Giulliano Alves da Costa
Beatriz de Faria Leão
Camilo Mussi
Gerson Zafalon Martins
José A. Escamilla
Mauricio Moreira
Ricardo Bessa

Sociedade Brasileira de Informática em Saúde

Diretoria Gestão 2007 -2008

Presidente: Heimar de Fátima Marin
Vice-Presidente: Evandro Eduardo Seron Ruiz
Secretária: Grace Dal Sasso
Tesoureiro: Cláudio Giulliano Alves da Costa

Membros do Grupo de Interesse (GI) em Certificação de Software e Padrões que participaram da elaboração deste manual

Adilson Eduardo Guelfi
Alex Souza Silveira
Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa (Coordenador)
Eduardo Pereira Marques
John Lemos Forman
Luis Gustavo Gasparini Kiatake
Luiz Renato Evangelisti
Matteo Nava
Marcelo Lúcio da Silva (Secretário)
Osni Pereira
Stanley da Costa Galvão (Vice-Coodenador)
Volnys Borges Bernal

Índice

Histórico das Revisões	5
Glossário	6
1. Introdução	7
2. Referencial Teórico	9
2.1. Definições	9
2.2. Padrões Utilizados	9
2.2.1. Resolução CFM No. 1638/2002.....	10
2.2.2. Resolução CFM No. 1639/2002.....	10
2.2.3. A Infra-estrutura de chaves públicas ICP-Brasil.....	11
2.2.4. Os Cadastros Nacionais em Saúde.....	11
2.2.5. O padrão TISS	11
2.2.6. Comissão Especial de Informática em Saúde da ABNT	12
2.2.7. Normas ISO TC-215.....	13
2.2.8. Normas ISO/IEC JTC1/SC27	13
2.2.9. ANSI HL7 Functional Model (EHR-S FM).....	13
2.2.10. Processo de Certificação CCHIT	14
3. Escopo de Certificação	15
3.1. Categorias dos Sistemas	16
4. Processo de Certificação	18
4.1. Etapas da Certificação	18
4.2. Credenciamento de Auditores.....	20
5. Requisitos de Conformidade	22
5.1. Visão Geral dos Requisitos de Segurança	22
5.2. Visão Geral dos Requisitos de Conteúdo, Estrutura e Funcionalidades	25
5.3. Visão Geral dos Requisitos TISS	26
5.4. Apresentação dos Requisitos para Certificação SBIS/CFM	27
5.5. Requisitos do Nível de Garantia de Segurança 1 (NGS1).....	28
5.6. Requisitos do Nível de Garantia de Segurança 2 (NGS2).....	37
5.7. Requisitos de Estrutura e Conteúdo.....	40
5.8. Requisitos de Funcionalidades	46
5.9. Requisitos TISS	54
6. Referências	65

Histórico das Revisões

Data	Versão	Descrição	Autores	Distribuição
25/08/2003	1.0	Especificação Inicial	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS
30/11/2003	1.1	Primeira Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
02/12/2003	1.2	Segunda Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
03/12/2003	1.3	Terceira Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
15/12/2003	1.4	Quarta Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
12/02/2004	2.0	Quinta Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
19/02/2004	2.1	Sexta Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	Público
12/09/2007	2.2	Início Revisão Fase 2	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
01/10/2007	2.3	Fase 2 – 2ª Revisão	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
04/10/2007	2.4	Fase 2 – 3ª Revisão	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
16/10/2007	2.5	Fase 2 – 4ª Revisão	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
16/10/2007	2.6	Revisão pré- consulta pública	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
19/10/2007	2.7	Revisão Final p/ consulta pública	Consultores SBIS	Consulta Pública
08/11/2007	3.0	Revisão Final p/ publicação	Consultores SBIS	Público

Glossário

ABNT – Associação Brasileira de Normas Técnicas
ABRAHUE – Associação Brasileira de Hospitais Universitários e de Ensino
AC – Autoridade Certificadora
AMB – Associação Médica Brasileira
ANS – Agência Nacional de Saúde Suplementar
ANSI – American National Standards Institute
ANVISA – Agência Nacional de Vigilância Sanitária
AR – Autoridade Registradora
ASSESPRO – Associação das Empresas Brasileiras de Tecnologia da Informação,
Software e Internet
CCHIT – Certification Commission for Healthcare Information Technology
CFM – Conselho Federal de Medicina
CNES – Cadastro Nacional de Estabelecimentos e Profissionais de Saúde do SUS
CNU – Cadastro Nacional de Usuários do SUS
CONARQ – Conselho Nacional de Arquivos
CRO – Conselho Regional de Odontologia
HL7 – Health Level 7
ICP – Infraestrutura de Chaves Públicas
IEC – International Engineering Consortium
ISO – International Standards Organization
ITI – Instituto Nacional de Tecnologia da Informação
MS – Ministério da Saúde
ONA – Organização Nacional de Acreditação
PEP – Prontuário Eletrônico do Paciente
RES – Registro Eletrônico em Saúde
SBIS – Sociedade Brasileira de Informática em Saúde
SGBD – Sistema de Gerenciamento de Banco de Dados
TISS – Troca de Informação em Saúde Suplementar
UTC – Coordinated Universal Time

1. Introdução

O Conselho Federal de Medicina (CFM) tem recebido nos últimos anos uma série de solicitações de pareceres a respeito da legalidade da utilização de sistemas informatizados para capturar, armazenar, manusear e transmitir dados do atendimento em saúde. Uma das indagações mais freqüentes é a substituição do papel pelo formato eletrônico. Cientes da complexidade do assunto e da necessidade de aprofundar os aspectos técnicos sobre esta questão, o CFM, através da Câmara Técnica de Informática em Saúde e Telemedicina, estabeleceu convênio de cooperação técnica com a Sociedade Brasileira de Informática em Saúde para desenvolver o processo de certificação de sistemas informatizados em saúde.

O primeiro produto da parceria SBIS/CFM foi a elaboração da resolução 1639/2002 que aprovava as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", dispondo sobre o tempo de guarda dos prontuários, estabelecendo critérios para certificação dos sistemas de informação e dando outras providências.

O segundo produto foi a elaboração do Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES). Com base neste manual, publicado em 2004 no sítio da SBIS e do CFM, teve início a Fase 1 do Processo de Certificação, e que até a presente data conta com mais de 70 sistemas auto-declarados (através de seus representantes legais) como estando aderentes ao conjunto de requisitos da versão 2.1 do Manual. A Fase 1 teve seu objetivo de preparar o mercado para o processo de Certificação, o que foi plenamente atingido.

A atualização deste Manual reflete o início da Fase 2 do Processo de Certificação SBIS/CFM, com a auditoria efetiva dos Sistemas de Registro Eletrônico em Saúde (S-RES). A atualização foi bastante abrangente, procurando refletir as experiências internacionais desenvolvidas desde 2004. Naquela ocasião não havia ainda no mundo um processo de certificação de S-RES em operação. Os EUA foram os primeiros a certificar S-RES, começando seu processo em 2006. Outros países ainda estão em fase de estudos e definições, sem sequer ter iniciado uma etapa de auto-certificação com requisitos já definidos.

Muito do que existia na versão 2.1 deste manual foi mantido, refletindo o cuidado e seriedade com que este trabalho vem sendo desenvolvido desde o seu início. Assim como na versão anterior, este documento contém o detalhamento dos requisitos de segurança, conteúdo e funcionalidades que um S-RES deve atender para receber o Selo de Qualidade SBIS/CFM. Alguns requisitos foram revistos e outros tantos incluídos, como é o caso dos requisitos relacionados com o TISS (ANS).

A auto-certificação (Fase 1) continuará sendo possível até que a SBIS tenha condições operacionais de iniciar as auditorias dos S-RES interessados em obter o selo SBIS/CFM. A previsão é que, no primeiro trimestre de 2008, a SBIS comece a receber oficialmente os formulários solicitando o agendamento das auditorias, substituindo todo o processo de auto-certificação (Fase 1). A lista de empresas que tenham se declarado em conformidade com a versão 2.1 do manual de requisitos continuará disponível para

consulta por um período de adaptação, ainda a ser determinado, mas que não será superior a seis meses. A idéia é dar oportunidade para que as empresas interessadas se organizem e possam submeter seus sistemas à auditoria, e também para que a SBIS tenha condições de atender todas as solicitações. Durante este período de adaptação, as empresas auditadas que receberem o selo SBIS-CFM (Fase 2) aparecerão com destaque no site da SBIS e, logo em seguida, serão apresentadas as empresas que haviam se auto-declarado em conformidade (Fase 1). Encerrado o período de adaptação, a lista de empresas auto-declaradas será retirada do site, permanecendo apenas aquelas que já tenham recebido o selo SBIS/CFM após uma auditoria bem-sucedida.

Este manual está organizado da seguinte forma:

- Capítulo 1 - Introdução
- Capítulo 2 - Referencial Teórico
- Capítulo 3 - Escopo de Certificação
- Capítulo 4 - Processo de Certificação
- Capítulo 5 - Requisitos e Conformidade
- Capítulo 6 - Referências

Cabe ainda esclarecer que o processo de certificação apresentado no capítulo 4 deste manual é minuciosamente detalhado no **Manual Operacional de Ensaios e Análises** (a ser publicado em breve), de leitura obrigatória para aqueles interessados em obter o selo de qualidade SBIS/CFM.

2. Referencial Teórico

A Certificação SBIS/CFM se baseia em conceitos e padrões internacionais da área de Informática em Saúde, muitos dos quais já foram traduzidos para o Português e reconhecidos como padrões brasileiros. Primeiramente apresentamos as definições de alguns termos indispensáveis para este manual, e em seguida fazemos um breve resumo dos principais padrões e iniciativas utilizados como referência na definição do processo e dos requisitos a serem observados nesta certificação.

2.1. Definições

O relatório técnico ISO/TR 20.514:2005 (ver em 2.2.7) apresenta uma série de definições importantes para a Informática em Saúde. Cabe destacar as seguintes definições:

- Registro Eletrônico de Saúde – **RES** – Um repositório de informação a respeito da saúde de indivíduos, numa forma processável eletronicamente.
- Sistemas de Registro Eletrônico de Saúde – **S-RES** – Sistema para registro, recuperação e manipulação das informações de um Registro Eletrônico de Saúde.

Como se pode observar, estas definições são propositalmente abrangentes. De qualquer modo, é importante lembrar que um S-RES pode englobar diversos sub-sistemas ou componentes.

Além dos componentes que implementam as funcionalidades de um S-RES (componente principal), em geral desenvolvido pela empresa requisitante desta avaliação,, podem existir componentes acessórios (ainda que indispensáveis) sobre os quais dependerá a implementação de diversas funcionalidades do sistema. Exemplos típicos são o sistema de gerenciamento de base de dados (SGBD), um componente dinâmico WEB (applet ou activeX), ou ainda um sistema de diretórios (ex. AD, LDAP, etc.) utilizado para armazenar parâmetros dos usuários, papéis e grupos. Um S-RES é o conjunto de todos estes sub-sistemas e módulos que são necessários para atender os requisitos especificados neste manual. Não faz parte do escopo da certificação, entretanto, certificar individualmente cada um destes sub-componentes, como por exemplo o SGDB ou o sistema operacional.

2.2. Padrões Utilizados

Segundo a Organização Internacional de Padronização (International Standards Organization - ISO), padrão é um documento estabelecido por consenso e aprovado por um grupo reconhecido, que estabelece para uso geral e repetido um conjunto de regras, protocolos ou características de processos com o objetivo de ordenar e organizar atividades em contextos específicos para o benefício de todos.

Sempre que possível, tornou-se como base padrões brasileiros na elaboração deste manual, com destaque para:

- as resoluções do CFM a respeito de prontuário do paciente;
- a Infra-Estrutura de Chaves Públicas Brasileiras – ICP Brasil, que dá validade aos documentos eletrônicos no País;
- os cadastros nacionais em Saúde; e
- o padrão TISS da ANS;

Além disto, estão sendo acompanhados os trabalhos desenvolvidos pela Comissão Especial de Informática em Saúde da ABNT e as iniciativas da organização HL7 Brasil.

Na ausência de padrões brasileiros, buscou-se padrões internacionais para complementar o trabalho sendo desenvolvido, destacando-se:

- Documentos do Comitê ISO/TC-215 Health Informatics:
 - ISO/TR 20.514:2005;
 - ISO/TS 18.308:2004;
 - ISO/DIS 27.799;
- Normas do ISO/IEC JTC1/SC27;
- ANSI HL7 Functional Model (EHR-S FM); e
- Processo de Certificação de Software da CCHIT.

Merece destaque o fato de que diferentes organizações, principalmente no âmbito internacional, estão desenvolvendo esforços para harmonizar padrões semelhantes que tenham sido elaborados por cada uma delas. É o caso, por exemplo, de alguns padrões criados pela ISO e que já se encontram no processo de serem harmonizados com o trabalho desenvolvido pela organização HL7.

A SBIS e o CFM estão atentos a esta tendência e observando os resultados que estão sendo gerados neste esforço de harmonização. Futuras versões deste manual deverão incorporar todos estes avanços. A seguir, apresenta-se com mais detalhes cada um dos padrões ou iniciativas acima mencionados.

2.2.1. Resolução CFM No. 1638/2002

A resolução CFM 1638/2002^[1] define prontuário médico e atribui as responsabilidades de preenchimento, guarda e manuseio do mesmo. Esta resolução torna obrigatória a existência de comissões de revisão de prontuários nos estabelecimentos de saúde onde se presta assistência médica, estabelecendo, as informações de caráter obrigatório que devem constar no prontuário, seja este eletrônico ou em papel.

2.2.2. Resolução CFM No. 1639/2002

A resolução CFM 1639/2002^[2] aprova as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", dispõe sobre tempo de guarda dos prontuários, estabelece critérios para certificação dos sistemas de informação. Esta resolução estabelece a guarda permanente para os prontuários médicos arquivados eletronicamente em meio óptico ou magnético, e microfilmados, bem como o prazo mínimo de 20 (vinte) anos para a preservação dos prontuários médicos em suporte de papel. Esta resolução foi o primeiro produto do Convênio SBIS/CFM para o estabelecimento da de Certificação de S-RES.

2.2.3. A Infra-estrutura de chaves públicas ICP-Brasil

A Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil foi criada através da Medida Provisória 2.200-2 de 24 de agosto de 2001^[3], transformando o Instituto Nacional de Tecnologia da Informação – ITI em autarquia ligada à Casa Civil da Presidência da República. Através desta MP e das resoluções publicadas pela ICP-Brasil, são estabelecidos os critérios para o estabelecimento e funcionamento do sistema, servindo de base para os serviços de assinatura, não-repúdio, identificação e sigilo. Como resultado, têm-se o aumento de segurança das transações eletrônicas e aplicações que façam uso de certificados digitais, assim como a possibilidade da migração total de processos em papel para meios eletrônicos, sem prejuízo do reconhecimento legal destes documentos. Mais informações podem ser obtidas em <http://www.icpbrasil.gov.br>.

2.2.4. Os Cadastros Nacionais em Saúde

Os principais cadastros nacionais são o Cadastro Nacional de Usuários do SUS ^[4] e o Cadastro Nacional de Estabelecimentos e Profissionais de Saúde - CNES^[5].

O Cadastro de Usuários (anteriormente chamado de Projeto Cartão Nacional de Saúde) estabelece o conjunto de informações necessárias para que uma pessoa seja identificada univocamente no sistema de saúde brasileiro. Hoje, existem no País 133 milhões de pessoas cadastradas na base federal.

Já o CNES estabelece a identificação unívoca de todos os estabelecimentos de saúde públicos e privados no País. O número CNES é de uso obrigatório na área pública e privada. O conjunto de dados de ambos os cadastros foi utilizado como padrão de identificação nos requisitos deste manual.

2.2.5. O padrão TISS

O padrão TISS - Troca de Informação em Saúde Suplementar^[6] é o padrão definido pela Agência Nacional de Saúde Suplementar - ANS (www.ans.gov.br) para registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde. O objetivo do padrão TISS é atingir a compatibilidade e interoperabilidade funcional e semântica entre os diversos sistemas independentes para fins de avaliação da assistência à saúde (caráter clínico, epidemiológico ou administrativo) e seus resultados, orientando o planejamento do setor.

O padrão TISS se divide em 4 categorias: conteúdo e estrutura, representação de conceitos em saúde, comunicação, e segurança e privacidade, conforme descrevem as Resoluções Normativas publicadas no site da ANS, na seguinte URL:

- http://www.ans.gov.br/portal/site/_hotsite_tiss/f_materia_21227.htm

A ANS determinou que as normas técnicas estabelecidas na Resolução CFM n.º 1639/2002 supracitada, e os requisitos do Nível de Garantia de Segurança 1 (NGS1) deste manual (ver 5.5) devem obrigatoriamente ser observados no padrão TISS. Para as entidades que utilizam webservices como padrão de comunicação é recomendada a

utilização do Nível de Garantia de Segurança 2 (NGS2) também descrito neste Manual (ver 5.6). Ressalta-se que a eliminação do papel só é possível por meio do cumprimento do NGS2.

Como poderá ser no capítulo 3, no escopo da certificação SBIS/CFM foi estabelecida uma categoria específica que engloba todo e qualquer sistema que apresente entre as suas funcionalidades a capacidade de ser uma das pontas em um canal de comunicação entre operadoras de planos de saúde e prestadores da assistência em saúde. Deste modo, qualquer S-RES poderá se submeter ao processo de certificação visando apenas validar sua aderência ao padrão TISS.

2.2.6. Comissão Especial de Informática em Saúde da ABNT

A ABNT - Associação Brasileira de Normas Técnicas (www.abnt.org.br) é a representante oficial do Brasil junto à ISO. Em outubro de 2006 a ABNT criou a Comissão Especial de Estudos em Informática em Saúde, inspirada no Comitê de Informática em Saúde da ISO, também conhecido como TC-215. A criação desta comissão é um marco importante para o desenvolvimento da área de padrões em saúde no Brasil, estando estruturada nos mesmos moldes do TC-215, com os seguintes Grupos de Trabalho - GT:

GT 1 – Modelos – concentra-se no estudo dos modelos e padrões de conteúdo para representar a informação em saúde. Os documentos ISO/TS 20.154:2005 e ISO/TR 18.308:2004, utilizados como marcos referenciais do processo de certificação, foram contribuições do GT 1 do Comitê ISO-TC-215. O GT 1 da Comissão Brasileira já traduziu estes dois documentos que serão submetidos à ABNT e a comunidade para também se tornarem padrões nacionais.

GT 2 - Interoperabilidade – concentra-se nos padrões para estabelecer a comunicação efetiva entre sistemas e equipamentos na área da saúde. É um dos grupos mais ativos no Comitê ISO com vários padrões aprovados. No Brasil, este grupo tem se dedicado as questões específicas da área de Telemedicina.

GT 3 – Conceitos – concentra-se nas terminologias em saúde. O trabalho é extenso e no Brasil o grupo já traduziu dois documentos de referência sobre o tema de terminologias e indicadores em saúde.

GT 4 – Segurança – concentra-se nos padrões de segurança da informação em saúde. A questão da assinatura digital e privacidade é um dos temas em discussão. No Brasil este grupo tem trabalhado e colaborado com a ISO 27.799, norma internacional de segurança da informação em Saúde, norma que será publicada quase que simultaneamente em Português e em Inglês.

Todos os padrões em discussão pela Comissão Especial de Estudos em Informática em Saúde da ABNT foram e serão, cada vez mais, os documentos de referência para este processo de certificação.

2.2.7. Normas ISO TC-215

A norma ISO/TR 20.514:2005^[7] é um documento de referência técnica (“TR -Technical Reference”) que estabelece as definições de RES e de Sistemas de RES. Esta norma descreve as principais categorias de sistemas, define cenários de utilização, e a necessidade de interoperabilidade semântica entre os diferentes S-RES. Adicionalmente esta norma introduz o conceito de Registro Pessoal de Saúde – RPS. O documento 20.514:2005 é um marco referencial na área de RES e S-RES e representa vários anos de trabalho na área de padrões para S-RES.

A norma ISO/TS 18.308:2004^[8] é um documento formal de especificação técnica (“TS – Technical Specification”) que define os requisitos para um S-RES. A norma apresenta os requisitos categorizados em estrutura, processo, comunicação, privacidade e segurança, médico-legal, ético, consumidor/cultural e também os requisitos relacionados à evolução de sistemas de RES.

O projeto de norma [ISO/DIS 27.799](#) “Health informatics -- Information security management in health using ISO/IEC 17.799”, que está em fase final para publicação, detalha e destaca a importância do emprego dos controles de segurança descritos na ISO/IEC 27.002^[14] com foco na área de saúde.

2.2.8. Normas ISO/IEC JTC1/SC27

O Joint Technical Committee 1 (JTC1) é o comitê técnico da ISO responsável pela elaboração de normas sobre tecnologia da informação. Seu subcomitê 27 (SC27) é responsável pelas normas que tratam das técnicas de segurança em tecnologia da informação. Desta forma, várias normas são de interesse também para a área de saúde, destacando-se as apresentadas a seguir.

A norma ISO/IEC 27.002:2005 “Information technology - Security techniques - Code of practice for information security management”^[14], comumente conhecida por sua antiga numeração ISO/IEC 17.799, é a norma mais difundida mundialmente no assunto segurança e apresenta os principais controles de segurança a serem empregados por qualquer instituição com o objetivo de proteger suas informações. Essa norma possui sua versão brasileira NBR ISO/IEC 27.002:2005 “Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação”^[15].

A norma ISO/IEC [15.408:2005](#) “Information technology -- Security techniques - Evaluation criteria for IT security” em suas três partes: “Part 1: Introduction and general model”^[16], “Part 2: Security functional requirements”^[17] e “Part 3: Security assurance requirements”^[18], descreve um processo e requisitos específicos para certificação de segurança de sistemas.

2.2.9. ANSI HL7 Functional Model (EHR-S FM)

O HL7 é o mais utilizado padrão para intercâmbio de dados na área da saúde no cenário internacional, há mais de 15 anos. Hoje, na versão 3.0, o padrão incorpora um modelo de referência RIM – Reference Information Model com conceitos de domínio clínico e administrativo^[9].

Em 2001 o HL7 estabeleceu um grupo de trabalho em Registros Eletrônicos em Saúde (EHR-SIG). Este grupo de trabalho definiu um conjunto de requisitos funcionais para S-RES: o EHR Funcional Model^[10]. O trabalho realizado por este comitê é extenso e cobre diferentes perfis de sistema, com um enfoque prático e proposta de scripts para validação dos requisitos.

No Brasil, em fevereiro de 2007, foi criado o Instituto HL7 Brasil a fim de dar respaldo jurídico e administrativo às atividades da representação do HL7 no Brasil (www.hl7brazil.org), com o intuito de "promover e prover padrões relacionados com a troca, integração, compartilhamento e recuperação de informação eletrônica, para apoio da prática médica e administrativa, permitindo um maior controle dos serviços de saúde". Os grupos de trabalho estão em fase de organização, dentre eles, o Grupo de Registro Eletrônico de Saúde e Registro Pessoal em Saúde, que discutem os requisitos funcionais de S-RES.

2.2.10. Processo de Certificação CCHIT

A Certification Commission for Healthcare Information Technology – CCHIT desenvolveu o processo de certificação de S-RES^[11] adotado no mercado americano. Sua origem é posterior à Certificação SBIS-CFM, já que foi criado em 2005 com um aporte inicial da ordem de 7.5 milhões de dólares, sendo administrado pelas seguintes organizações:

- American Health Information Management Association (AHIMA);
- Healthcare Information and Management Systems Society (HIMSS); e
- National Alliance for Healthcare Information Technology (the Alliance).

O processo americano é voluntário e baseado em conjuntos de scripts para diferentes categorias de S-RES. Inicialmente apenas sistemas ambulatoriais podiam ser certificados, mas a CCHIT está expandindo as categorias de sistemas que podem se submeter ao processo de certificação. Os critérios são bastante detalhados e analisam a funcionalidade, conteúdo, estrutura, segurança e aspectos de interoperabilidade dos S-RES. Os S-RES são avaliados por três auditores, à distância, a partir de ambiente cooperativo especializado para esta finalidade. O processo do ponto de vista técnico é semelhante ao da SBIS/CFM.

3. Escopo de Certificação

O processo de Certificação SBIS/CFM destina-se, genericamente, a Sistemas de Registro Eletrônico de Saúde (S-RES). Como já visto na seção 2.1. , a definição do que é um S-RES é bastante ampla e abrangente, englobando todos os subsistemas e componentes (SGBDs, servidores, bibliotecas, etc.). Será avaliado o conjunto completo de subsistemas e componentes que compõem o S-RES, devidamente configurados de forma a atender os requisitos especificados neste manual.

Desta forma, qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde pode ser considerado como sendo um S-RES. Tendo em vista a existência de um grande número de S-RES no mercado brasileiro, englobando uma ampla faixa de sistemas focados em diferentes nichos do mercado de saúde, não seria possível, num primeiro momento, certificar todo e qualquer S-RES existente.

Inicialmente o processo de Certificação SBIS/CFM estará disponível apenas para algumas categorias mais genéricas de S-RES. No futuro próximo, e considerando a demanda futura, as categorias poderão ser ampliadas, e em alguns casos, especializadas.

É importante ressaltar que é dever do desenvolvedor do S-RES, independentemente da categoria de S-RES em que este se enquadra, indicar para seus usuários e clientes todas as interdependências entre cada um dos subsistemas e componentes necessários para que o S-RES seja configurado e funcione de maneira correta, especialmente quando estes subsistemas ou componentes não são fornecidos juntamente com o S-RES, cabendo ao usuário/cliente tratar o licenciamento destes junto à terceiros.

É imprescindível que a documentação do S-RES indique o nome e versão de cada um de seus subsistemas ou componentes, bem como o local onde os mesmos podem ser obtidos (seja junto a um fornecedor comercial, seja o repositório de um projeto de software livre). Além disso, devem ser informadas todas as instruções sobre a configuração necessária para o correto funcionamento destes subsistemas/componentes em conjunto. Todas estas informações devem ter como referência o nome e versão do sistema operacional sobre o qual irão funcionar.

3.1. Categorias dos Sistemas

Para fins da Certificação SBIS/CFM, inicialmente, poderão ser submetidos ao processo de certificação apenas os S-RES enquadrados em uma das categorias abaixo:

- a) **Assistencial** – sistemas voltados para a assistência, ou seja, todo o S-RES que registra atendimentos em saúde, tais como: sistemas de automação de consultórios clínicos, sistemas de informação hospitalar e ambulatorial, sistemas de vigilância epidemiológica, etc.;
- b) **SADT** – sistemas de apoio diagnóstico e terapêutica, tais como: automação de laboratório, emissão de laudos, imagens médicas, e outros;
- c) **GED** – sistemas de gerenciamento eletrônico de documentos, utilizados para o armazenamento e visualização de documentos relacionados à informação de saúde;
- d) **TISS** – criada para atender ao padrão TISS da ANS. Inúmeros S-RES, especialmente aqueles em uso por operadoras de planos de saúde e prestadores de assistência em saúde, são obrigados a trocar informações usando o TISS.

Qualquer sistema que queira obter o selo SBIS/CFM deverá fazer uma solicitação formal à SBIS para dar início ao processo de certificação (ver capítulo 4). Neste momento, a pessoa ou organização interessadas, deverão indicar em quais categorias o seu sistema se enquadra.

Sistemas voltados para consultórios médicos provavelmente se enquadrarão apenas na categoria Assistencial, mas um grande sistema hospitalar integrado poderá apresentar características e funcionalidades que atendam não apenas à categoria Assistencial, mas também às categorias SADT e GED. Um sistema como este provavelmente estará apto ainda a trocar informações utilizando o TISS, e neste caso, poderá ser solicitada a certificação em todas as categorias acima.

Como poderá ser visto adiante, no capítulo 5, a certificação SBIS/CFM prevê ainda níveis diferenciados nos requisitos de segurança. Está prevista a possibilidade de um S-RES ser enquadrado em dois níveis distintos de garantia de segurança, sendo o primeiro nível bastante amplo, enquanto o segundo nível engloba todos os requisitos do primeiro nível e ainda exige que o S-RES tenha as funcionalidades necessárias para trabalhar com certificados digitais padrão ICP-Brasil. Adicionalmente, o S-RES deverá ser identificado como sendo um S-RES local ou um S-RES remoto, refletindo se o mesmo funciona isoladamente ou se pode ser acessado simultaneamente por diferentes usuários a partir de estações de trabalho conectadas ao computador onde o S-RES está instalado.

Para ser aprovado, um S-RES precisará necessariamente se enquadrar em pelo menos uma das categorias de S-RES descritas acima, atendendo todos os requisitos

estabelecidos para aquela categoria, além de atender também todos os requisitos previstos pelo menos no Nível de Garantia de Segurança 1 (NGS1).

A Tabela 1 abaixo exibe as diferentes combinações possíveis de certificação, de acordo com a categoria de S-RES.

Tabela 1 – Tipos de certificação conforme categoria de S-RES

Categoria de Sistema	Tipo de Certificação
Sistemas Assistenciais	ASSIST + NGS1
	ASSIST + NGS1 + TISS
	ASSIST + NGS2
	ASSIST + NGS2 + TISS
Sistemas SADT	SADT + NGS1
	SADT + NGS1 + TISS
	SADT + NGS2
	SADT + NGS2 + TISS
GED	GED + NGS1
	GED + NGS2
TISS	TISS + NGS1
	TISS + NGS2

Conforme já mencionado anteriormente, admite-se também a certificação combinada das categorias ASSISTENCIAL, SADT e GED, especialmente no caso de sistemas integrados.

Caberá ao interessado na certificação de um S-RES indicar as categorias de sistema, nível de garantia de segurança e se o S-RES é local ou remoto, para que estas informações sejam consideradas no processo de certificação. A categoria TISS admite também algumas variações nos requisitos, de acordo com sub-categorias específicas, conforme detalhado na seção 5.3. .

4. Processo de Certificação

Tais como os processos de acreditação hospitalar e/ou certificações ISO, a Certificação SBIS-CFM estabelece que a auditoria seja realizada por equipe especializada, que verifica se, realmente, os requisitos obrigatórios para a categoria selecionada são atendidos pelo S-RES.

Como se trata de software (programa de computador), essa auditoria corresponde, na prática, a uma bateria de testes na qual o sistema é amplamente analisado por um grupo de auditores, devidamente treinados, credenciados e selecionados pela SBIS, todos membros titulares da Sociedade.

Em linhas gerais, uma pessoa ou instituição interessada em certificar o seu sistema (proponente), deve seguir as etapas abaixo:

- a) analisar a documentação sobre o processo de certificação disponível no site da SBIS;
- b) verificar se o S-RES a ser certificado realmente atende a todos os requisitos obrigatórios para a categoria desejada (os requisitos de segurança são obrigatórios para qualquer categoria);
- c) realizar a bateria de testes internamente em sua instituição, conforme descrito no Manual Operacional de Ensaios e Análises. Este manual estará em breve disponível no site da SBIS e poderá ser baixado pelo próprio Proponente;
- d) cumpridas as etapas anteriores, estando o proponente seguro que o seu S-RES esta em condições de ser aprovado na auditoria, somente então ele deverá iniciar formalmente o processo para obtenção do selo de qualidade SBIS/CFM conforme descrito a seguir.

4.1. Etapas da Certificação

Apresentam-se abaixo os principais passos do processo geral da Certificação SBIS-CFM (veja resumo na Figura 1 - Processo de Certificação).

A) Proponente solicita a Certificação do software no site da SBIS

No site da SBIS, o Proponente deve preencher o pedido de avaliação inicial, informando os dados do desenvolvedor (instituição/empresa), características do sistema, bem como tecnologias e subsistemas utilizados. É importante que estas informações sejam corretamente preenchidas já que servirão de subsídio para elaboração da proposta de trabalho com o respectivo orçamento.

B) SBIS envia orçamento de auditoria

A partir dos dados informados, a SBIS envia ao Proponente o seu plano de trabalho e orçamento para auditoria, levando em consideração na elaboração dos mesmos, as categorias e nível de segurança para os quais esta sendo solicitada a auditoria do S-RES.

C) Proponente analisa orçamento

Com o plano de trabalho e orçamento, o Proponente irá aprovar ou não a realização da auditoria. Caso o Proponente não aprove, a solicitação será então arquivada pela SBIS. Caso aprove, o Proponente deve comunicar à SBIS a aceitação da auditoria, acessando o site e confirmando a solicitação. A SBIS irá então preparar e enviar o contrato de serviços.

D) Proponente efetua o pagamento da primeira parcela da Certificação

Após assinatura do contrato de serviços entre as partes, a SBIS envia o boleto para o Proponente pagar a primeira parcela do valor acordado para a Certificação.

E) SBIS seleciona a equipe de auditores

Com a confirmação do pagamento da primeira parcela pelo Proponente, a SBIS seleciona os auditores que irão analisar o S-RES do Proponente, a partir do banco de consultores treinados e credenciados pela Sociedade (os critérios para a seleção dos auditores podem ser visto em 4.2). A SBIS envia a relação de auditores e data de início da auditoria com o respectivo cronograma de trabalho.

F) Proponente analisa auditores e cronograma

O Proponente analisa a relação de auditores e as datas propostas e, não havendo conflito de interesses, nem inviabilidade de datas e horários, confirma a realização da auditoria. Caso não possa realizar a auditoria nas datas propostas, o Proponente deve comunicar à SBIS já sugerindo datas alternativas. O proponente poderá também solicitar a substituição de um ou mais auditores indicados pela SBIS, que irá analisar as justificativas apresentadas e só então enviará novas opções de auditores. Estando de acordo com os auditores e data propostas, o proponente deve fazer o pagamento da parcela restante do montante acordado para a auditoria.

G) Auditores realizam análise do sistema

Com a confirmação do pagamento da parcela restante pelo Proponente, e seguindo o cronograma e plano de trabalho, os auditores iniciam a análise do S-RES. Para isso, o submetem a uma bateria de testes. Todos os auditores seguem o mesmo plano de testes. Para cada item de teste realizado, os auditores devem indicar se o mesmo foi ou não verificado (atendeu ou falhou).

H) Auditores comunicam à SBIS o resultado final

Ao final da auditoria os auditores informarão à SBIS o resultado dos testes realizados. Para isso, responderão questionário interno disponível em área reservada no site da SBIS, similar ao plano de testes, indicando se o sistema foi aprovado ou não. Se o S-RES foi realmente aprovado, um novo boleto é emitido relativo à taxa de registro e emissão do Certificado SBIS/CFM.

I) Proponente efetua o pagamento da taxa de certificado

O Proponente deve efetuar o pagamento da taxa para que assim a SBIS emita o certificado e divulgue a aprovação do S-RES na auditoria para o público em geral.

J) SBIS emite o certificado e publica no site

Com o pagamento da taxa, o Certificado é gerado em forma eletrônica, um arquivo PDF é enviado para o Proponente e publicado no site da Certificação. Além disso, um certificado em papel é enviado via correio para o endereço do Proponente.

No site da SBIS, todos os S-RES Certificados estarão publicados com os dados de contato da empresa, suas características e visualização do certificado em PDF.

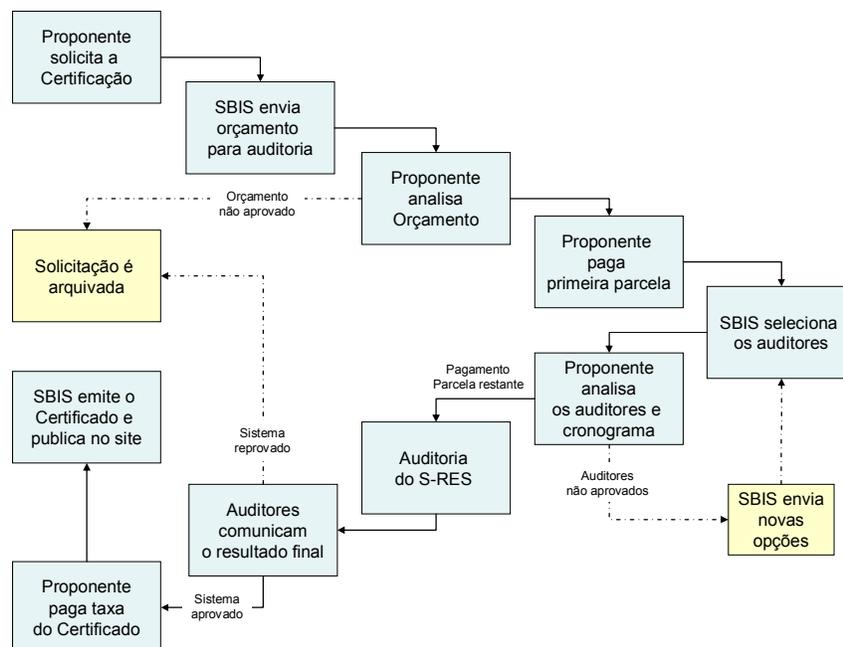


Figura 1 - Processo de Certificação SBIS-CFM

4.2. Credenciamento de Auditores

A SBIS é a instituição responsável por operacionalizar a Certificação no âmbito do convenio SBIS/CFM. Como tal, credencia auditores que irão efetivamente realizar a auditoria do S-RES, determinando se este atende ou não aos requisitos e, com isso, receber o Certificado.

Os critérios de seleção para que um profissional possa se tornar um auditor estão descritos abaixo:

1. ser “Membro Titular” da SBIS, e estar em dia com suas obrigações;
2. ter realizado e sido aprovado no “Curso Oficial da Certificação SBIS-CFM”;
3. estar vinculado a uma empresa associada à SBIS.

As empresas que desejam indicar auditores para participar do processo de certificação devem manifestar o seu interesse preenchendo o formulário indicado no site da Certificação. Adicionalmente, será também exigida a seguinte documentação:

- Cópia do Cartão do CNPJ
- Cópia do Contrato Social e Aditivos
- Dados da Pessoa de contato
- Para cada auditor deverá ser encaminhado um currículo conforme modelo encontrado no site da certificação, destacando para cada um deles a respectiva formação e experiências prévias em Certificações ISO, ONA ou certificações de segurança de software.

Esta documentação deverá ser encaminhada para a SBIS no endereço:

Sociedade Brasileira de Informática em Saúde
Rua Tenente Gomes Ribeiro No.57 - Sala 33
Vila Clementino
São Paulo-SP
CEP. 04038-040
Fone: (11) 3791-3343

Mais detalhes sobre o processo de certificação, credenciamento de auditores, e demais tópicos relacionados com este assunto poderão ser encontrados no Manual Operacional de Análises e Ensaios SBIS/CFM.

5. Requisitos de Conformidade

O principal objetivo da revisão deste manual foi atualizá-lo com as referências mais atuais na área de RES e S-RES, uma vez que os documentos utilizados no referencial teórico, em especial os do TC-215 da ISO sofreram modificações significativas desde 2004. Houve, também, a necessidade de incorporar o padrão TISS e as iniciativas do HL7 e CCHIT, entre outras. A lista com todos os padrões utilizados e uma descrição resumida de cada um deles está na seção 2.

Vários dos padrões utilizados como referência descrevem características e funcionalidades que idealmente devem estar presentes em S-RES, independentemente do seu nicho de aplicação.

As características e funcionalidades existentes em um padrão qualquer podem e devem ser utilizadas como base para facilitar a avaliação de um S-RES. Adicionalmente, podem ser úteis para o planejamento de novas versões de S-RES ao longo do tempo (incorporando características e funcionalidades existentes no padrão, mas ainda não disponíveis no sistema).

Já do ponto de vista do processo de certificação, é necessário estabelecer critérios objetivos que possam ser utilizados de modo uniforme em cada auditoria, garantindo que os S-RES avaliados tenham as mesmas chances de serem ou não aprovados no processo, independentemente dos auditores envolvidos.

Os requisitos mandatórios da certificação SBIS/CFM foram extraídos dos padrões de referência, buscando-se identificar aqueles mais adequados à realidade brasileira. Vários requisitos obrigatórios no cenário internacional foram definidos como opcionais nos requisitos da certificação. Estes devem ser vistos com funcionalidades e ou características desejáveis para futuros desenvolvimentos.

Os requisitos da certificação SBIS-CFM foram agrupados da seguinte forma:

- Requisitos de Segurança;
- Requisitos de Conteúdo, Estrutura e Funcionalidades; e
- Requisitos TISS

Nos itens seguintes, apresenta-se uma visão geral de cada um deles.

5.1. Visão Geral dos Requisitos de Segurança

Os requisitos de segurança de um S-RES são fundamentais para aqueles interessados em eliminar o registro em papel das informações relativas a cada paciente.

Existe uma série de recomendações quanto ao acesso, uso e armazenamento dos prontuários em papel, várias delas visando resguardar a sua legitimidade, ao mesmo tempo preservando a segurança e confidencialidade das informações ali contidas.

De forma análoga, os requisitos de segurança aqui apresentados buscam resguardar a legitimidade das informações manipuladas e armazenadas em um S-RES, ao mesmo tempo preservando a segurança e confidencialidade destas informações.

Os prontuários em papel estão sujeitos a falsificações, destruição (p.ex., incêndio ou inundação), além de extravio ou roubo. Com o prontuário em um S-RES não é diferente, sendo que muitos entendem que estes riscos são até maiores para um S-RES na medida em que computadores conectados à internet podem ser facilmente invadidos (maior risco de roubo e quebra de confidencialidade), se medidas adequadas de segurança não forem adotadas. Outro exemplo são sistemas incorretamente configurados, permitindo que usuários inexperientes possam equivocadamente formatar a unidade de disco onde o S-RES está instalado, perdendo todos os dados ali armazenados. O que fazer nesta situação? Os mais versados na informática poderão lembrar que um usuário cuidadoso deve sempre se preocupar em fazer cópias de segurança das informações armazenadas no computador (também conhecidas como “backup”).

Mas se os riscos são maiores para os prontuários eletrônicos, por outro lado a reversão de situações de risco é muito mais fácil em sistemas computadorizados. No exemplo acima, mesmo que o disco rígido do computador tenha entrado em curto-circuito, a existência de um “backup” recente permitirá a instalação do S-RES em um novo computador e a recuperação quase que imediata dos dados armazenados na cópia de segurança. Em pouco tempo o usuário pode voltar a utilizar o S-RES com perdas mínimas. Tamanha facilidade seria possível caso os prontuários estivessem em papel e fossem destruídos pelo fogo ?

Em outras palavras, tanto o prontuário em papel como o prontuário eletrônico estão sujeitos a riscos. Que fique claro, no entanto, que é praticamente impossível reduzir a zero os riscos envolvidos na utilização de prontuários, seja em papel ou em formato eletrônico. O usuário deve estar constantemente avaliando os riscos potenciais e decidindo por medidas preventivas de segurança que possam mitigar estes riscos. Os requisitos de segurança apresentados a seguir procuram orientar desenvolvedores de S-RES e seus respectivos usuários quanto aos cuidados mínimos que devem ser observados na utilização de sistemas computadorizados.

Quanto à decisão de abandonar o papel e passar a operar apenas com informações armazenadas em um S-RES, ela deve ser tomada avaliando os riscos envolvidos. A legislação brasileira deixa claro que a versão impressa de um documento eletrônico armazenada em um computador será considerada válida se todas as partes interessadas naquele documento reconhecerem sua legitimidade. Mas o que fazer se um paciente colocar em dúvida a validade de uma prescrição médica armazenada em um S-RES? Como provar que tal prescrição é verdadeira e que não foi adulterada para corrigir o valor de uma dosagem que, segundo o paciente, era diferente na versão que foi originalmente a ele entregue?

Uma alternativa é a contratação de um perito técnico para analisar o sistema computadorizado e as práticas de segurança adotadas em seu uso, emitindo parecer sobre a validade ou não daquela prescrição. Trata-se de um procedimento custoso, muitas vezes demorado, e que dependendo das características do S-RES poderá ser inconclusivo.

Uma outra alternativa, amparada pela legislação brasileira, é ter assinado digitalmente tal prescrição, usando para tanto um certificado digital em conformidade com a ICP-Brasil. Neste caso, qualquer documento eletrônico será considerado válido, para todos os efeitos, inclusive perante tribunais brasileiros, como tendo sido assinado pela pessoa ou instituição para a qual o certificado digital foi emitido.

Assim sendo, a prescrição médica sendo contestada em nosso exemplo, mesmo que tenha sido gerada no computador por um editor de textos qualquer, mas que tenha sido assinada digitalmente pelo médico que a criou, terá o mesmo valor legal que uma prescrição escrita e assinada manualmente no receituário deste mesmo médico.

Não custa lembrar, entretanto, que documentos eletrônicos, mesmo quando assinados digitalmente, precisam observar cuidados adicionais de segurança. De nada adiantará assinar digitalmente as informações de um S-RES se tais informações não forem submetidas a “backups” periódicos, garantindo que continuarão a existir e estarão disponíveis no futuro caso vierem a ter sua legitimidade questionada.

Em função deste cenário, o processo de certificação SBIS/CFM classifica os S-RES, do ponto de vista de segurança da informação, em dois Níveis de Garantia de Segurança (NGS):

- **NGS1** - categoria constituída por S-RES que *não* contemplam o uso de certificados digitais ICP-Brasil para assinatura digital das informações clínicas, conseqüentemente sem amparo para a eliminação do papel e com a necessidade de impressão e aposição manuscrita da assinatura;
- **NGS2** - categoria constituída por S-RES que viabilizam a eliminação do papel nos processos de registros de saúde. Para isso, especifica a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação. Para atingir o NGS2 é necessário que o S-RES atenda aos requisitos já descritos para o NGS1 e apresente ainda total conformidade com os requisitos especificados para o nível de garantia 2.

Recomenda-se, para ambos os níveis, a observância das boas práticas para a gestão da segurança da informação descritas na norma NBR ISO/IEC 27.002^[15] publicada pela ABNT, adaptadas as necessidades organizacionais de cada instalação do S-RES.

A certificação SBIS/CFM considera no seu processo de auditoria o nível de segurança para o qual o S-RES se declara em conformidade, já que o NGS2 incorpora todos os requisitos do NGS1, e prevê um conjunto adicional de requisitos.

Os S-RES auditados no NGS1 devem possuir todas as características necessárias para que uma perícia técnica possa tirar conclusões satisfatórias sobre a validade ou não das informações por ele armazenadas. As conclusões da perícia deverão levar em consideração também a forma como o sistema está sendo utilizado, já que o S-RES, por si só, não será suficiente para garantir a legitimidade de qualquer informação. Um exemplo para tornar mais clara esta afirmação é aquele em que o S-RES possui mecanismos para validar seus usuários através de identificação e senha, mas este

mecanismo se torna irrelevante na medida em que todos os usuários do sistema usam a mesma identificação e senha para acessar o sistema.

Já os S-RES auditados no NGS2, estarão em condições de gerar documentos eletrônicos assinados digitalmente em conformidade com a ICP-Brasil. Tais documentos serão considerados válidos independentemente de auditoria, mas, novamente, o S-RES apenas permitirá que os documentos sejam assinados. O uso efetivo de certificados digitais, em conjunto com a observância dos demais requisitos de segurança, dependerá também da forma como o S-RES for utilizado por seus usuários.

Finalmente, dependendo de como o S-RES pode ser acessado pelos seus usuários, requisitos diferenciados de segurança devem ser considerados. Para efeito da certificação SBIS/CFM, consideramos como **S-RES de acesso local** todo e qualquer S-RES no qual o usuário só consegue acessar e utilizar o sistema a partir do mesmo computador onde ele (e todos os seus subsistemas e componentes) está instalado. Além disso, um S-RES de acesso local não permite o acesso simultâneo de mais de um usuário. Por outro lado, o **S-RES de acesso remoto** é todo e qualquer S-RES que permite o acesso simultâneo ao sistema, e independentemente de estarem fazendo este acesso do próprio computador onde o S-RES está instalado, ou de um computador remoto via algum tipo de conexão (rede local, conexão sem-fio, internet, etc.).

Para as instituições que queiram deixar de usar o prontuário em papel, a SBIS e o CFM recomendam a opção pelos S-RES certificados como NGS2, ao mesmo tempo buscando uma certificação de aderência à Norma ABN NBR ISO/IEC 27.001:2006^[19], oferecida por várias empresas do mercado.

A avaliação dos riscos envolvidos deve ser feita por cada instituição, cabendo somente a elas decidir sobre o grau de equilíbrio entre custo e risco que esteja mais adequado às suas necessidades e possibilidades.

5.2. Visão Geral dos Requisitos de Conteúdo, Estrutura e Funcionalidades

Hoje são ainda poucos os S-RES no Brasil que atendem a vários dos requisitos listados neste manual, como por exemplo, a incorporação de alertas, diretrizes e protocolos clínicos. Entretanto, a SBIS e o CFM entendem que as definições do comitê técnico ISO TC-215 definem requisitos importantes para um S-RES, sempre buscando apoiar e facilitar a atividade assistencial. Neste primeiro momento vários requisitos foram considerados apenas como desejáveis (e não obrigatórios), mas espera-se que futuramente todos os S-RES incorporem funcionalidades mais sofisticadas.

As características de funcionalidades de um S-RES variam de acordo com a finalidade do sistema. Por este motivo os requisitos de funcionalidades dependem da categoria do S-RES (ver seção 3).

5.3. Visão Geral dos Requisitos TISS

Os requisitos específicos para verificar a aderência ao padrão TISS refletem o conteúdo da RN 153, de 29/05/2007, da ANS. Os requisitos foram agrupados em conteúdo, estrutura e comunicação de dados, para que assim um sistema possa ser considerado em conformidade com o TISS.

Além disto, é preciso distinguir se o S-RES tem como foco a automação de operadoras de planos de saúde (médico e/ou odontológico) ou a automação de prestadores de serviços de saúde (categorias 1, 2 e 3). Esta sub-divisão respeitou a categorização adotada pela ANS, no cronograma de implantação do TISS, melhor detalhada na Tabela 2 a seguir.

Tabela 2. Categorias de prestadores e operadoras para a implantação do TISS.

	Prestadores	Operadoras
Grupo 1	<ul style="list-style-type: none"> ▪ hospitais gerais ▪ hospitais especializados ▪ hospitais/dia-isolado ▪ pronto socorro especializado ▪ pronto socorro geral ▪ clínica especializada / ambulatório de especialidade ▪ unidade de apoio à diagnose e terapia (SADT isolado) ▪ unidade móvel de nível pré-hospitalar - urgência/emergência ▪ unidade móvel fluvial ▪ unidade móvel terrestre ▪ policlínica 	Operadoras de planos de assistência médica
Grupo 2	<ul style="list-style-type: none"> ▪ consultório isolado ▪ profissionais de saúde ou pessoa jurídica que presta serviço em consultório médico 	
Grupo 3	<ul style="list-style-type: none"> ▪ clínica radiológica em odontologia ▪ consultório odontológico isolado ▪ odontólogo ou pessoa jurídica da área odontológica que presta serviço em consultório 	Operadoras de planos Odontológicos

Cabe ainda lembrar que na definição dos requisitos de conteúdo e estrutura para S-RES utilizados por prestadores de serviços pertencentes ao Grupo 1, foi ainda necessário distinguir entre S-RES para SADTs isolados, e S-RES para todos os demais tipos de instituição contidos neste grupo.

O conjunto de requisitos obrigatórios do TISS na certificação são definidos de acordo com o enquadramento do S-RES na Tabela 2.

Finalmente, qualquer sistema que se submeta ao processo de certificação na categoria TISS terá que necessariamente atender pelo menos os requisitos do nível de garantia de segurança 1 (seção 5.5.).

5.4. Apresentação dos Requisitos para Certificação SBIS/CFM

Nas próximas páginas, serão apresentados cada um dos requisitos considerados na certificação SBIS/CFM. Para cada requisito, são apresentadas as seguintes informações:

- ID – Identificação do requisito, utilizando codificação padronizada.
- NOME DO REQUISITO.
- REFERÊNCIA – identificação da função ou característica existente em um padrão de referência e que deu origem a este requisito.
- CONFORMIDADE – descrição do requisito, incluindo exemplos sempre que apropriado. Aqui podem também ser fornecidas indicações de como o requisito será avaliado durante a auditoria visando à certificação SBIS/CFM.
- PRESENÇA – Indicação se o requisito é:
 - **Mandatário (M)** – Deve ser obrigatoriamente atendido pelo S-RES;
 - **Recomendado (R)** – É importante levar em conta este requisito, recomendando-se fortemente que os desenvolvedores de S-RES que não atendam o mesmo comecem a planejar seu respectivo desenvolvimento;
 - **Opcional (O)** – Requisitos opcionais, que não serão considerados no processo de certificação;
 - **Não se aplica (X)** - É possível se deparar com a situação em que não faz sentido observar se um determinado requisito é atendido ou não. Nestes casos, ao invés de deixar o campo em branco, suscitando dúvidas, o mesmo será preenchido com a letra **X**, indicando que não se deve considerar tal requisito para a categoria ou tipo de S-RES correspondente.

Para alguns requisitos a coluna PRESENÇA estará subdividida, considerando tipos ou sub-categorias de S-RES. É o que se observa nos requisitos de Conteúdo, Estrutura e Funcionalidades, onde temos as seguintes colunas:

- **A** – Assistencial
- **S** – SADT
- **G** – GED

Já nos requisitos de segurança, em alguns requisitos a coluna PRESENÇA está dividida entre LOCAL e REMOTO, refletindo como cada requisito deverá ser considerado de acordo com o tipo do S-RES que está sendo auditado.

5.5. Requisitos do Nível de Garantia de Segurança 1 (NGS1)

NGS1.01 - Controle de versão do software

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.01.01	Versão software	HL7 ERH-S FM IN4.2 ABNT NBR ISO/IEC 27001:2006 A.12.5	Todos os componentes do S-RES devem possuir versão do software associada a uma única referência (nome, fornecedor e número de versão) e não ambígua. O S-RES deve permitir a exibição da versão de seus componentes de software para todos os usuários.	M	M
NGS1.01.02	Código fonte	HL7 ERH-S FM IN5.2 ABNT NBR ISO/IEC 27001:2006 A.12.5	Deve ser possível, a partir do número de versão de cada componente do S-RES, resgatar os códigos-fonte correspondentes, possibilitando a rastreabilidade dos arquivos fontes que o geraram.	R	R
NGS1.01.03	Histórico de alteração	HL7 ERH-S FM IN4.2	Manter histórico descritivo de todas as alterações realizadas em cada versão, contendo a data e o responsável pela alteração.	R	R
NGS1.01.04	Repositório de versões	HL7 ERH-S FM IN4.2	Ter um repositório estruturado com todas as versões dos componentes (executáveis e códigos-fonte) que foram utilizadas em produção em algum momento, permitindo voltar versões anteriores em casos de atualizações mal sucedidas.	R	R
NGS1.01.05	Dependências dos componentes	HL7 ERH-S FM IN5.2	Para cada versão de cada componente, indicar no manual de instalação e requisitos de sistema quais são as dependências com outros componentes do S-RES ou do ambiente, e os requisitos de operação. Por exemplo, informar que uma determinada versão de componente é compatível com o padrão HL7 versão 2.x (requisito de operação), que roda em um determinado sistema operacional (requisito de ambiente), que depende de um específico sistema de diretório para autenticação de usuários.	R	R

NGS1.02 - Identificação e autenticação de usuário

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.02.01	Identificação e autenticação do usuário	HL7 ERH-S FM IN1.1; ABNT NBR ISO/IEC 27001:2006 A.11.5.2	Todo usuário deve ser identificado e autenticado antes de qualquer acesso a dados do S-RES.	M	M
NGS1.02.02	Método de autenticação	HL7 ERH-S FM IN1.1 ABNT NBR ISO/IEC 27001:2006 A.11.5.1	Utilizar métodos tradicionais de autenticação, como usuário/senha, ou métodos mais seguros, como certificação digital, One Time Password (OTP) ou biometria.	M	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.02.03	Proteção dos parâmetros de autenticação	SBIS	Todos os dados ou parâmetros utilizados no processo de autenticação de usuário devem ser armazenados de forma protegida. Por exemplo, o armazenamento do código <i>hash</i> da senha do usuário ao invés dela própria, além disso, o local de armazenamento desse código <i>hash</i> deve possuir restrições de acesso; na autenticação via OTP, a semente utilizada deve ser protegida.	M	M
NGS1.02.04	Segurança de senhas	ABNT NBR ISO/IEC 27001:2006 A.11.5.3	Quando a autenticação for baseada em usuário/senha, utilizar os seguintes controles de segurança: <ul style="list-style-type: none"> • Qualidade da senha: verificar a qualidade 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; • Periodicidade de troca de senhas: o S-RES deve ter funcionalidade de obrigar a troca de senhas pelos usuários, em um período máximo configurável; • Não armazenar a senha, somente o código <i>hash</i> das senhas do usuário. • 	M	M
NGS1.02.05	Controle de tentativas de login	ABNT NBR ISO/IEC 27001:2006 A.11.5.1	O S-RES deve ter mecanismos para bloquear o usuário após um número máximo configurável de tentativas inválidas de <i>login</i> .	M	M

NGS1.03 - Controle de sessão de usuário

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.03.01	Encerramento por inatividade	ABNT NBR ISO/IEC 27001:2006 A.11.5.5	Sessão de usuário (local ou remota) inativa deve ser encerrada após um período definido de inatividade.	M	M
NGS1.03.02	Segurança contra roubo de sessão de usuário	ABNT NBR ISO/IEC 27001:2006 A.10.8	Em S-RES distribuído a sessão de comunicação deve possuir controles de segurança a fim de não permitir o roubo da sessão do usuário. O roubo de sessão de comunicação pode ocorrer, inclusive em sessões protegidas (ex. SSL/TLS). Por exemplo, se o controle de sessão for realizado através de <i>cookie</i> na URL, em determinadas situações, a URL da sessão de um usuário pode ser obtida e utilizada por um outro usuário, personificando o usuário anterior.	X	M

NGS1.04 - Autorização e controle de acesso

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NSG1.04.01	Impedir acesso por entidades não autorizadas	HL7 ERH-S FM IN1.2 ABNT NBR ISO/IEC 27001:2006 A.11.6.1	Impedir acesso ao RES (acesso direto à base de dados) e ao S-RES por entidades (usuários ou outros sistemas) não autenticadas e não autorizadas.	M	M
NSG1.04.02	Mecanismo de controle de acesso ao RES	HL7 ERH-S FM IN1.2	Garantir que o acesso ao RES seja somente possível através do mecanismo de controle de acesso, mesmo para o administrador do sistema ou outro usuário que porventura venha a ter acesso ao RES.	M	M
NSG1.04.03	Gerenciamento de usuários	HL7 ERH-S FM IN1.2 ISO/TS 18308:2004(E) PRS3.2	Permitir o gerenciamento de usuários (criação, remoção e modificação), gerenciamento de papéis (criação, remoção e modificação) e gerenciamento de grupos (criação, remoção e modificação).	M	M
NSG1.04.04	Papéis relacionados à TI	SBIS	Suportar os seguintes papéis relacionados à tecnologia da informação (não obrigatoriamente com tais nomes): <ul style="list-style-type: none"> • Gestor de segurança; • Auditor; • Administrador do sistema; • Operador do sistema; • Operador de backup: exportação de dados para fins de cópia (Backup). Mesmo que o S-RES não possua funções para realização de backup, sendo o sistema de gerenciamento da base de dados (SGBD) um componente do S-RES, deve existir no SGBD o perfil de operador de backup. 	R	M
NSG1.04.05	Configuração de controle de acesso	HL7 ERH-S FM IN1.2; ABNT NBR ISO/IEC 27001:2006 A.11.6 ISO/TS 18308:2004(E) PRS3.3	Disponibilizar mecanismos necessários para que seja possível implementar a política de controle de acesso através da configuração dos perfis de acesso, considerando os papéis de usuário, dos grupos e das operações que podem ser realizadas, inclusive a diferenciação de operações de consulta e de inclusão/alteração. Considerar que um mesmo usuário pode possuir mais de um papel.	M	M
NSG1.04.06	Concessão de autorizações	HL7 ERH-S FM IN1.2	Disponibilizar ao gestor de segurança meios para conceder autorizações aos usuários e controle de acesso aos recursos de acordo com o escopo de atuação, a política organizacional e legislação.	M	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NSG1.04.07	Delegação de poder	SBIS	<p>Sendo o atribuidor aquele responsável por autorizar a delegação de poder e o delegado aquele quem recebe a delegação de poder, então:</p> <ul style="list-style-type: none"> • O atribuidor deve ser previamente autorizado para conceder tais classes de autorização; • A delegação de poder deve ser registrada no sistema; • A delegação de poder deve informar: <ul style="list-style-type: none"> • O atribuidor; • O delegado; • O motivo • O instante da concessão • O período de vigência <p>Como exemplo de delegação pode-se citar um médico que delega poder de entrada de informações ao RES de um paciente para uma enfermeira.</p>	M	M
NSG1.04.08	Acesso ao RES pelo paciente.	HL7 ERH-S FM IN1.4	<p>Garantir que o paciente possa ter acesso a todas as suas informações pessoais e clínicas armazenadas no S-RES. Caso o S-RES não permita acesso direto do próprio paciente ao S-RES, deve existir um papel de usuário que permita realizar esta atividade em nome do paciente. Esta atividade deve ser registrada (log), devendo ser informado: o usuário, o paciente, o local e o instante da operação. O usuário deverá poder levar consigo estas informações em formato eletrônico ou impresso. O sistema deverá disponibilizar uma interface para impressão de declaração do usuário de que está recebendo suas informações, contendo o nome do paciente, nome do usuário do sistema que está exportando ou imprimindo os dados, local e instante da operação.</p>	M	M
NSG1.04.09	Restrições de acesso ao RES adicionadas pelo paciente	HL7 ERH-S FM IN1.4	<p>Permitir que o paciente possa adicionar restrições de acesso a uma determinada parte ou à totalidade de seu RES.</p>	O	O

NGS1.05 - Disponibilidade do RES

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.05.01	Cópia de Segurança	ABNT NBR ISO/IEC 27001:2006 A.10.5	<p>O S-RES deve permitir que a salvaguarda dos dados e o arquivamento atendam aos seguintes requisitos:</p> <ul style="list-style-type: none"> • exportar os atributos de segurança em conjunto com os dados; • garantir na restauração de uma cópia de segurança e arquivamento que os atributos de segurança e suas associações sejam automaticamente 	M	M

			recuperados, sem a intervenção do administrador; <ul style="list-style-type: none"> assegurar que somente o usuário com papel de operador de backup possa exportar e restaurar uma cópia de segurança e arquivamento; 		
NGS1.05.02	Verificação de integridade na recuperação de dados	ABNT NBR ISO/IEC 27001:2006 A.10.5	A salvaguarda de dados (backup) deve incluir controles para verificação da integridade dos dados. Garantir a verificação da integridade dos dados armazenados no RES, sempre que houver recuperação da informação	M	M

NGS1.06 - Comunicação remota

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.06.01	Segurança da comunicação entre cliente e servidor	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES de acesso remoto, a sessão de comunicação entre o componente cliente (do lado do usuário) e o componente servidor deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados. Como exemplo, pode-se citar a utilização do protocolo HTTPS (HTTP + SSL/TLS).	X	M
NGS1.06.02	Controle de acesso do cliente ao servidor	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES de acesso remoto, o acesso ao sistema deve ser restrito somente aos clientes previamente autorizados. Este controle de acesso pode ser realizado, por exemplo, pelo endereço IP do cliente.	X	R
NGS1.06.03	Restrição de dados transmitidos	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES de acesso remoto os dados transmitidos ao componente cliente (lado do usuário) devem ser somente aqueles que serão apresentados ao usuário. Ou seja, todo e qualquer processamento relacionado à seleção de dados deve ser realizado no lado servidor.	X	M
NGS1.06.04	Segurança da comunicação entre componentes	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES composto por diversos componentes distribuídos (localizados em computadores diferentes), a comunicação entre tais componentes (como, por exemplo, com o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação de parceiro (cliente e servidor), integridade dos dados e confidencialidade dos dados.	X	M
NGS1.06.05	Controle de acesso entre componentes	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES composto por diversos componentes distribuídos (localizados em computadores diferentes), na comunicação entre tais componentes (como, por exemplo, com o banco de dados), o acesso ao componente deve ser restrito somente aos parceiros (componentes) previamente autorizados.	X	M
NGS1.06.06	Comunicação entre S-RES.	HL7 ERH-S FM IN1.7	O canal de comunicação entre S-RES deve oferecer os seguintes serviços de segurança: autenticação de parceiro (cliente e servidor), integridade dos dados e confidencialidade dos dados. Quando a comunicação envolva S-RES de diferentes entidades, a autenticação de parceiro deve utilizar certificados digitais ICP-Brasil.	M	M

NGS1.07 - Segurança de Dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.07.01	Importação de dados	HL7 ERH-S FM IN1.6	Os dados importados de outro S-RES devem estar relacionados a um paciente e um médico responsável, local e momento (data e hora) da importação e profissional usuário do sistema que realiza a importação.	M	M
NGS1.07.02	Restrições para transmissão e exportação de RES	SBIS	A transmissão e exportação de RES de um S-RES deve ser permitida somente nas seguintes situações: <ul style="list-style-type: none"> • para transmissão para um outro S-RES; • para salvaguarda de dados (backup); • para arquivamento; • para o paciente, a pedido do paciente, podendo ser realizada de forma eletrônica ou por impressa; • em processos internos nos quais seja necessária a impressão de parte do RES; • para atendimento ao requisito legal de manter documentação em papel, através da impressão; Todas as atividades de transmissão de RES devem ser registradas (logs).	M	M
NGS1.07.03	Impedir exclusão e alteração	SBIS	Não permitir exclusão ou alteração de dados já existentes no RES. Ações de correção devem preservar os dados antigos.	M	M
NGS1.07.04	Verificação de integridade dos dados	SBIS	Devem existir controles para verificação de integridade dos dados RES de forma a prevenir que qualquer ação do usuário ou falha do sistema possa originar uma inconsistência nos dados. Este requisito pode ser atendido pelo SGBD utilizado pelo S-RES.	R	R
NGS1.07.05	Utilização de SGBD	SBIS	O RES deve ser protegido por um Sistema de Gerenciamento de Banco de Dados.	M	M
NGS1.07.06	Impedir acesso direto ao SGBD	SBIS	O SGBD não deve permitir acesso direto pelos usuários. O acesso de usuários ao RES deve ser permitido somente por intermédio do componente de autenticação e controle de acesso do S-RES, nunca diretamente pelo SGBD, exceto nas atividades de salvaguarda (backup) de dados	M	M
NGS1.07.07	Dados de identificação do paciente criptografados	SBIS	Os dados de identificação do paciente devem ser criptografados a fim de impedir a reconstrução do seu RES através de acessos não autorizados à base de dados do S-RES ou à cópia de segurança (gerado na salvaguarda dos dados). Este requisito pode ser atendido pelo SGBD utilizado pelo S-RES.	R	R
NGS1.07.08	Confirmação de entrega	SBIS	A troca de dados entre S-RES, caso do TISS, deve possuir controles de confirmação de entrega/recebimento dos dados.	M	M

NGS1.08 – Auditoria

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.08.01	Auditoria de acesso	ISO/TS 18308:2004(E) PRS5.1	Suportar o registro de dados para auditoria de acesso e modificação de dados em parte ou no todo do S-RES	M	M
NGS1.08.02	Integridade das trilhas de auditoria	ABNT NBR ISO/IEC 27001:2006 A.10.10.3	Os recursos e informações de registros (log) devem ser protegidos contra falsificação e acesso não autorizado. Trilhas de auditoria não podem ser modificadas por nenhum usuário.	M	M
NGS1.08.03	Acesso às trilhas de auditoria	ABNT NBR ISO/IEC 27001:2006 A.10.10.1	Garantir que o acesso às trilhas de auditoria somente seja permitida a usuário com papel Auditor.	M	M
NGS1.08.04	Trilha de auditoria	ABNT NBR ISO/IEC 27001:2006 A.10.10.1 ISO/TS 18308:2004(E) PRS5.3	A trilha de auditoria deve conter eventos relacionados a: <ul style="list-style-type: none"> • tentativas de autenticação de usuário; • atividades de gerenciamento de usuários, papéis e grupos; • atividades de administração do sistema; • atividades de operação do sistema; • operações realizadas pelos usuários; • interação com outros sistemas, incluindo outros S-RES; • troca (transmissão e recepção) de dados; • salvaguarda de dados; • arquivamento de dados; • acessos à base de dados; • erros do S-RES; • alertas de incidentes de segurança; 	M	M

NGS1.09 - Documentação

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.09.01	Documentação	SBIS	Possuir as seguintes documentações: <ul style="list-style-type: none"> • Manual de instalação e requisitos de sistemas; • Manual do usuário; • Manual do administrador e operador; • Manual de mecanismos de segurança; • Manual de práticas de segurança. 	M	M
NGS1.09.02	Referência à versão do software na documentação	SBIS	Todos os manuais devem indicar claramente, no início do documento, a versão a que se referem.	M	M
NGS1.09.03	Alteração Documentação	SBIS	Informar e manter histórico de todas as alterações nos manuais, para que o usuário possa consultar todas as alterações realizadas até a última versão disponível.	O	O
NGS1.09.04	Operador de backup	ABNT NBR ISO/IEC 27001:2006	O manual de instalação deve informar como realizar a configuração de um usuário com perfil de operador de backup no SGBD. Além disso, O manual de instalação deve informar como configurar o SGBD de forma que as atividades de exportação e restauração de uma cópia de segurança (backup) dos dados possa ser realizada somente pelo usuário com papel de operador de backup.	R	R
NGS1.09.05	Restrição de acesso a entidades não autenticadas e autorizadas	SBIS	O manual de instalação deve informar como configurar o SGBD de forma a impedir o acesso de entidades (usuários ou outros sistemas) não autenticadas e não autorizadas pelo componente de autenticação e controle de acesso do S-RES.	R	R
NGS1.09.06	Verificação da integridade dos dados	SBIS	O manual de instalação e operação deve informar que, quando houver recuperação de salvaguarda de dados, o sistema deve realizar a verificação da integridade dos dados.	R	R
NGS1.09.07	Configuração da Segurança da comunicação entre componentes	SBIS	O manual de instalação e operação deve informar que a comunicação entre os componentes de um S-RES distribuído deve implementar os serviços de segurança de autenticação de parceiro (cliente e servidor), integridade dos dados e confidencialidade dos dados, caso tais componentes não estiverem em uma rede segregada da Internet e dos demais ambientes, principalmente daqueles em que estão os usuários, assim como dos componentes que acessam diretamente a web.	X	M
NGS1.09.08	Sincronização de relógio	ABNT NBR ISO/IEC 27001:2006 10.10	O manual de administração e operação deve informar ao administrador que os componentes do S-RES devem estar com seus relógios sincronizados ao UTC. O manual deve também informar as formas para que a sincronização possa ser configurada no ambiente.	O	R

NGS1.10 - Tempo

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.10.1	Representação de instante de tempo	ISO 8601:1998	Toda informação de tempo deve ser armazenada com referência ao UTC com indicação do fuso local. As referências de instante de tempo podem ser apresentadas ao usuário em formatos de hora local	M	M
NGS1.10.2	Formato de representação de tempo	ISO 8601:1998	Toda informação de instante de tempo deve ser representada (armazenada ou transmitida) no formato da ISO 8601, com exceção do carimbo de tempo, que segue RFC 3161	O	O

NGS1.11 – Notificação de Ocorrências

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.12.01	Interface para notificação	ABNT NBR ISO/IEC 27002:2006 13.1.1	Disponibilizar uma interface para que usuários possam notificar sobre ocorrência de incidentes de segurança, problemas, melhoramentos ou sugestões.	O	R

5.6. Requisitos do Nível de Garantia de Segurança 2 (NGS2)

NGS2.01 – Certificação Digital

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS2.01.01	Certificado digital	ICP-Brasil; Resolução CFM	Utilização de certificado digital emitido por AC credenciada à ICP-Brasil para os processos de autenticação de profissionais e para assinatura digital documentos eletrônicos no S-RES.	M	M
NGS2.01.02	Atendimento à ICP e PC	ICP-Brasil; Resolução CFM	Atender às normas de uso definidas pela ICP-Brasil e pela “Política de Certificado” (PC) na utilização de certificados digitais.	M	M
NGS2.01.03	Validação do certificado digital antes do uso	ICP-Brasil	Antes da utilização de qualquer certificado digital deve ser realizada sua verificação e a adequação de seu propósito de uso. A verificação do certificado digital envolve a validação criptográfica, verificação de validade, verificação de revogação, inclusive dos certificados da sua cadeia de certificação.	M	M
NGS2.01.04	Configuração de certificados raiz	ICP-Brasil	Permitir a configuração do conjunto de certificados raiz de confiança. Deve, também, possuir controles para garantia da integridade desta informação.	M	M

NGS2.02 – Assinatura Digital

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS2.02.01	Formato de assinatura	SBIS	Utilizar formatos abertos a fim de garantir a interoperabilidade dos dados. Neste sentido, a assinatura digital deverá utilizar estruturas compatíveis com o formato CMS [RFC 3852] ou XMLDSIG [RFC 3275]	M	M
NGS2.02.02	Verificação do certificado digital	ETSI TS 101 733	Verificar, antes da realização de uma assinatura digital, o certificado digital a ser utilizado e adequação de seu propósito de uso à assinatura digital	M	M
NGS2.02.03	Referência temporal para revogação	ETSI TS 101 733	Toda assinatura digital realizada no âmbito do S-RES deve incluir um carimbo de tempo (RFC 3161) que deve ser utilizado como referência temporal nas atividades de verificação de revogação.	R	R
NGS2.02.04	Validação da assinatura digital	SBIS	Realizar a validação da assinatura digital após sua realização.	M	M
NGS2.02.05	Validação da	ETSI TS 101 733	Manter os elementos necessários (informações sobre domínios de segurança, cadeia	M	M

	assinatura a qualquer momento		de certificados e informações de revogação) a fim de possibilitar que a assinatura digital possa ser validada a qualquer momento futuro.		
NGS2.02.06	Propósito da assinatura e papel do signatário	ETSI TS 101 733	Incluir, em toda assinatura digital realizada, o propósito da assinatura (tipo de comprometimento que o signatário assume no momento de firmar a assinatura digital) e o papel do signatário no S-RES.	M	M
NGS2.02.07	Visualização das informações assinadas	SBIS	Sempre permitir a visualização da informação a ser assinada e garantir que seja realizada exatamente sobre as mesmas informações visualizadas.	M	M
NGS2.02.08	Homologação ICP-Brasil	ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para assinatura digital devem ser homologados pela ICP-Brasil.	R	R

NGS2.03 – Autenticação de usuário utilizando certificado digital

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS2.03.01	Verificação do certificado digital para autenticação	ICP-Brasil	Antes da realização de uma assinatura digital, verificar o certificado digital a ser utilizado e a adequação de seu propósito de uso à autenticação do usuário.	M	M
NGS2.03.02	Irretratabilidade da autenticação realizada	SBIS	A autenticação realizada através de certificado digital deve gerar prova de forma a garantir a irretratabilidade da autenticação realizada. O elemento de prova deve ser armazenado em registros de segurança do sistema.	M	M
NGS2.03.03	Homologação ICP-Brasil	ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para autenticação devem ser homologados pela ICP-Brasil.	R	R

NGS2.04 – Digitalização de Documentos (Considerar apenas para S-RES da categoria GED)

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
NGS2.04.01	Assinatura digital do documento digitalizado pelo software.	SBIS	Todo componente de digitalização deve possuir um par de chaves assimétricas e certificado digital associado. Todo documento digitalizado deve ser assinado pelo componente de digitalização com esta chave.	R
NGS2.04.02	Assinatura digital do documento digitalizado pelo operador.	SBIS	O operador de digitalização deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil tipo A3 ou A4, utilizando o propósito “garantia de origem”. O propósito de garantia de origem pode ser estabelecido incluindo o atributo assinado “commitment-type-indication” com o propósito genérico “id-cti-etc-proofOfOrigin”.	M
NGS2.04.03	Assinatura pelo responsável ou conferente	Resolução CFM;	O responsável ou conferente deve também assinar digitalmente o documento digitalizado, com certificado ICP-Brasil tipo A3 ou A4 utilizando o propósito “conferência”. O propósito de conferência pode ser estabelecido incluindo o atributo assinado “commitment-type-indication” com o propósito genérico “id-cti-ets-proofOfReceipt”, enquanto não seja definido um propósito mais específico.	M
NGS2.04.04	Classificação	SBIS	Possuir capacidade de classificar os documentos digitalizados para possibilitar o agrupamento	M
NGS2.04.05	Indexação	Resolução CFM;	Todo documento digitalizado deve possuir informações mínimas de indexação, como tipo, assunto, data.	M
NGS2.04.06	Qualidade	Resolução CFM;	O documento digitalizado deve reproduzir todas as informações dos documentos originais	M
NGS2.04.07	Instante da assinatura.	SBIS	Toda assinatura de documento digitalizado deve incluir o atributo signing-time, contendo o instante da assinatura no formato UTC.	M
NGS2.04.08	Termo de conduta para digitalização	SBIS	Permitir ao usuário a realização de operações de digitalização somente após a assinatura digital do “Termo de conduta para digitalização” que deve conter requisitos sobre confidencialidade das informações e sobre a responsabilidade do processo.	M
NGS2.04.09	Homologação ICP-Brasil	ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para assinatura digital devem ser homologados pela ICP-Brasil.	R

5.7. Requisitos de Estrutura e Conteúdo

ESTR.01 - Estrutura do RES

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.01.01	Navegação e consultas	ISO STR1.1 TS 18308:2004(E)	Possibilitar que a informação do RES esteja organizada em diferentes seções que devem se refletir nos mecanismos de navegação e consultas	M	M	M
ESTR.01.02	Estrutura mínima	ISO STR1.2 TS 18308:2004(E) CFM 1638/2002	Assegurar que o formato do RES está aderente ao conjunto de especificações estabelecidas pela resolução 1638/2002 do CFM, aos padrões de identificação de usuário, profissional e estabelecimento conforme descritos no Cadastro Nacional de Usuários, e adotados no projeto piloto do Cartão Nacional de Saúde (www.saude.gov.br/cartao), e no Cadastro Nacional de Estabelecimentos de Saúde (www.datasus.gov.br/cnes). Para a área de saúde privada, os requisitos de informação da ANS (www.ans.gov.br) devem ser garantidos	M	M	M
ESTR.01.03	Independência	ISO STR1.3 TS 18308:2004(E)	Suportar o compartilhamento de RES com independência de hardware, software (aplicativos, Sistemas operacionais, linguagens de programação), bancos de dados, redes, sistemas de codificação e linguagens naturais	R	R	R
ESTR.01.04	Recuperação de dados	ISO STR1.4 TS 18308:2004(E)	Possibilitar que a informação seja organizada e recuperada de tal forma que facilite os usos secundários do RES, tais como: vigilância epidemiológica, gestão, faturamento e pesquisa	R	R	R
ESTR.01.05	Armazenamento do RES	ISO STR1.5 TS 18308:2004(E)	Suportar armazenamento do RES	M	M	M

ESTR.02 - Dados estruturados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.02.01	Armazenamento em listas	ISO STR2.1 TS 18308:2004(E)	Permitir armazenamento de dados em listas, de tal forma que a ordem cronológica seja preservada sempre que a informação for apresentada	M	M	M
ESTR.02.02	Preservação de relacionamento de dados	ISO STR2.2 TS 18308:2004(E)	Permitir o armazenamento de dados em tabelas de tal forma que os relacionamentos dos dados com as linhas e colunas seja preservado	M	M	M
ESTR.02.03	Hierarquia de nodos	ISO STR2.3 TS 18308:2004(E)	Permitir o armazenamento de dados em hierarquias, preservando o relacionamento dos nodos pais com os nodos filhos	M	M	M
ESTR.02.04	Associação do nome e valor dado	ISO STR2.4 TS 18308:2004(E)	Possibilitar o armazenamento de dados simples, preservando a associação entre nome do dado e respectivo valor.	M	M	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.02.05	Armazenamento de múltiplos valores	ISO STR2.5 TS 18308:2004(E)	Possibilitar o armazenamento de múltiplos valores para a mesma observação coletada seqüencialmente, em curtos intervalos de tempo, durante um mesmo contato ou em diferentes contatos e locais. O contexto no qual as medidas foram realizadas deve ser preservado, como, o tipo de ferramenta e metodologia utilizada e quem a coletou. Estes valores devem ser retornados quando solicitado, e ordenados de diferentes formas.	M	M	M
ESTR.020.6	Texto livre	ISO STR2.6 TS 18308:2004(E) ERH-S FM- IN 2.5.1	Suportar a inclusão de texto livre	M	M	M
ESTR.02.07	Busca e inclusão	ISO STR2.7 TS 18308:2004(E)	Suportar busca em dados estruturados e não-estruturados e a inclusão de texto estruturado nesses dados	M	M	M
ESTR.02.08	Inclusão de comentários	ISO STR2.8 TS 18308:2004(E)	Possibilitar a inclusão de comentários nos dados armazenados, desta forma permitindo ao médico clarificar a informação estruturada apropriadamente. Deve ser possível associar os comentários com os respectivos dados (atributos)	R	R	R
ESTR.02.09	Ênfase nos comentários e dados	ISO STR2.9 TS 18308:2004(E)	Oferecer mecanismos que possibilitem ao profissional de saúde expressar ênfase nos comentários ou dados fornecidos. Dependendo do tipo de ênfase, a forma como os dados são apresentados após uma consulta pode ser modificada.	R	R	R

ESTR.03 - Dados Administrativos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.03.01	Registro de identificação do paciente	ISO STR2.11 TS 18308:2004(E) SUS	Incorporar o registro da identificação do paciente, localização, dados demográficos, pessoa para contato, dados ocupacionais e outros dados administrativos.	M	M	M
ESTR.03.02	Padrões do CNS, CNES, CNPJ	ISO STR2.12 TS 18308:2004(E) SUS	Adotar padrões para representar de forma não ambígua o sujeito da atenção, os profissionais (de saúde ou não) envolvidos no processo assistencial incluindo seus papéis no contexto da assistência, local da assistência, data e hora inicial e final do processo assistencial. Para identificação do usuário e do profissional responsável pelo atendimento e pela digitação dos dados utilizar os padrões de identificação do Cartão Nacional de Saúde. Para a identificação do Estabelecimento Assistencial de Saúde (EAS) utilizar código do Cadastro Nacional de Estabelecimentos de Saúde – CNES. Em se tratando de consultórios particulares que não possuam o número CNES utilizar o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), ou a identificação do profissional responsável conforme padrões do Cartão Nacional de Saúde.	M	M	M
ESTR.03.03	Episódios de atenção	ISO STR2.13 TS 18308:2004(E)	Gerenciar a administração dos processos em saúde e episódios de atenção, bem como a organização de cada encontro e seus dados	M	M	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.03.04	Informações financeiras e comerciais	ISO STR2.14 TS 18308:2004(E)	Registrar as informações financeiras ou comerciais tais como planos de saúde e respectivas elegibilidades, coberturas, responsável por despesas, custos, taxas e utilização	R	R	R
EST3R.03.05	Situação legal	ISO STR2.15 TS 18308:2004(E)	Registrar a situação legal e consentimentos relevantes para o cuidado do paciente (ex: situação legal do guardião, consentimento para cirurgia e outros procedimentos)	R	R	R
ESTR.03.06	Vigilância	ISO STR2.16 TS 18308:2004(E)	Oferecer consultas e relatórios para atender às demandas da vigilância epidemiológica, sanitária e doenças de notificação compulsória	M	M	M

ESTR.04 - Dados clínicos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
REST.04.01	Dados estruturados ou não	ISO STR2.10 TS 18308:2004(E) SUS	Registrar, armazenar e recuperar dados estruturados e não estruturados sobre: <ul style="list-style-type: none"> ▪ Anamnese (história do paciente) ▪ Exame físico ▪ Antecedentes mórbidos pessoais (psicológicos, sociais, ambientais) e familiares ▪ Alergias e outras informações de relevância clínica ▪ Imunizações e medidas preventivas e outras intervenções no estilo de vida ▪ Investigação diagnóstica, intervenções terapêuticas tais como medicamentos e procedimentos ▪ Evoluções clínicas, interpretações, decisões e raciocínio clínico ▪ Solicitação de exames, tratamentos e encaminhamentos ▪ Hipóteses Diagnósticas, Lista de Problemas, Diagnósticos, Questões relevantes, preferências e expectativas ▪ Consentimentos informados (desejável) ▪ Plano de saúde ▪ Sumário de alta com as condições funcionais e de saúde ▪ Informações a respeito de próteses ou implantes: fornecedor, modelo 	M	O	O
ESTR.04.02	Laudos e resultados de exames	ISO STR2.10 TS 18308:2004(E) SUS	Suportar laudos e resultados de exames, com a descrição do que foi realizado, método utilizado, data e hora da realização, profissional responsável pelo laudo/resultado e conclusão	R	M	O
ESTR.04.03	Envio eletrônico de dados	ISO STR2.10 TS 18308:2004(E) SUS	Atender as exigências de envio eletrônico de dados de faturamento, produção, e vigilância conforme as normas do SUS / Ministério da Saúde e Agência Nacional de Saúde Suplementar	R	R	R

ESTR.05 - Tipos de dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.05.01	Dados numéricos e quantificáveis	ISO STR3.1 TS 18308:2004(E)	Representar dados numéricos e quantificáveis Definir a estrutura lógica de dados numéricos e quantificáveis, incluindo o gerenciamento de unidades	M	M	M
ESTR.05.02	Precisão da medida	ISO STR3.2 TS 18308:2004(E)	Informar o grau de precisão da medida realizada	R	M	R
ESTR.05.03	Porcentagem e valor absoluto	ISO STR3.3 TS 18308:2004(E)	Expressar as porcentagens também em valores absolutos	R	M	R
ESTR.05.04	Limites	ISO STR3.4 TS 18308:2004(E)	Incorporar a definição de limites inferior e superior adequados ao contexto clínico	M	M	R
ESTR.05.05	Lógica dos valores fracionados	ISO STR3.5 TS 18308:2004(E)	Possibilitar a representação lógica dos valores fracionados	R	M	R
ESTR.05.06	Lógica de data e hora	ISO STR3.6 TS 18308:2004(E)	Incorporar a definição da estrutura lógica de valores data e hora	M	M	M
ESTR.05.07	Definições incompletas	ISO STR3.7 TS 18308:2004(E)	Aceitar definições incompletas ou aproximadas de data e hora, tais como: - datas aproximadas – ex: ontem; semana passada - datas parciais – ex: ??/Maio/1997; ??/??/1928	M	M	R
ESTR.05.08	Eventos e ações futuras	ISO STR3.8 TS 18308:2004(E)	Registrar eventos ou ações futuras, tais como: - Períodos do dia ou de tempo: manhã, tarde, noite, enquanto acordado; - Momentos aproximados de datas ou horas: ao acordar, durante as refeições (café da manhã, almoço, jantar), ao deitar; - Momentos relativos de datas ou horas: antes do café da manhã, após o almoço, dois dias após a alta, uma semana depois da última dose; - Períodos alternados de datas/horas: alternadamente a cada 8 horas, todas as segundas, quartas e sextas-feiras, todos os domingos, toda terceira terça-feira	R	R	R
ESTR.05.09	Linha de tempo	ISO STR3.9 TS 18308:2004(E)	Registrar a hora de um dado momento, o tempo decorrido desde um evento em particular, e a duração (data hora de início e data hora fim)	R	R	R
ESTR.05.10	Fuso horário	ISO STR3.10 TS 18308:2004(E)	Registrar o fuso horário do local onde o registro foi realizado	R	R	R
ESTR.05.11	Precisão de milissegundos	ISO STR3.11 TS 18308:2004(E)	Registrar as unidades de tempo com precisão de milissegundos	M	M	R
ESTR.05.12	DICOM, MIME e ECG	ISO STR3.12 TS 18308:2004(E)	Suportar a representação de tipos de dados padronizados, tais como: DICOM, MIME e ECG	R	R	R

ESTR.06 - Dados de referência

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.06.01	Dados de referência	ISO STR3.13 TS 18308:2004(E)	Registrar dados de referência, tais como valores normais, e os atributos e contexto relevantes a uma observação ou medida em particular	M	M	R

ESTR.07 - Dados contextuais

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.07.01	Eventos já ocorridos	ISO STR3.14 TS 18308:2004(E)	Suportar o registro de dados contextuais associados a data/hora de eventos já ocorridos	M	M	R
ESTR.07.02	Contexto e tempo	ISO STR3.15 TS 18308:2004(E)	Suportar o registro de dados contextuais associados a data/hora de eventos relacionados com o registro	M	M	R
ESTR.07.03	Contexto e assunto	ISO STR3.16 TS 18308:2004(E)	Suportar o registro de dados contextuais associados ao assunto	M	M	R
ESTR.07.04	Contexto e responsável	ISO STR3.17 TS 18308:2004(E)	Suportar o registro de dados contextuais associados à pessoa responsável pelo registro e ocorrência do registro	M	M	R
ESTR.07.05	Contexto e ambiente físico	ISO STR3.18 TS 18308:2004(E)	Suportar o registro de dados contextuais associados à estrutura física do ambiente onde ocorreu o cuidado a saúde	M	M	R
ESTR.07.06	Contexto e localização	ISO STR3.19 TS 18308:2004(E)	Suportar o registro de dados contextuais associados com a localização onde o evento foi registrado	M	M	R
ESTR.07.07	Contexto e razão	ISO STR3.20 TS 18308:2004(E)	Suportar o registro de dados contextuais associados à razão do registro da informação associada ao evento	M	M	R
ESTR.07.08	Contexto e protocolo	ISO STR3.21 TS 18308:2004(E)	Suportar registro de dados contextuais associados ao protocolo associado à informação registrada	M	M	R

ESTR.08 - Associações

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.08.01	Associação semântica	ISO STR3.22 TS 18308:2004(E)	Representar a associação semântica dos links entre diferentes informações no RES	R	R	R
ESTR.08.02	Dados referenciados externamente	ISO STR3.23 TS 18308:2004(E)	Suportar as associações de “dados referenciados externamente” para aqueles dados que não puderem ser representados no RES, desde que a segurança do paciente não seja comprometida	M	M	M

ESTR.09 - Representação de conceitos em saúde

Este grupo de requisitos se presta a garantir que haja registro dos conceitos em saúde preservando a forma originalmente informada, bem como sua representação no(s) sistema (s) de codificação escolhido(s), como por exemplo, SNOMED e/ou CID. Este expediente garante a decodificação dos conceitos por futuros sistemas de codificação, a partir da informação original e não a codificada. Por exemplo, numa história patológica progressiva, a informação de que o paciente teve "sarampo na infância complicado com pneumonia" deve ser registrada nos formatos originais e codificados, informando o(s) código(s) e versão do sistema de codificação.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
ESTR.09.01	Múltiplos sistemas de codificação	ISO STR 4.1 TS 18308:2004(E)	Suportar os múltiplos sistemas de codificação (terminologias de entrada ou interface, terminologia de referência, e classificações) através de interfaces com ferramentas eletrônicas, tais como: navegadores de terminologia, editores e servidores de vocabulários.	R	R	R
ESTR.09.02	Captura de código	ISO STR4.2 TS 18308:2004(E) HL7 CNS	Suportar ao nível do atributo para captura de código, o esquema de codificação (ex: sistema de classificação ou codificação), versão, idioma original e descrição original	M	M	M
ESTR.09.03	Vocabulário padrão e de origem	ISO STR4.3 TS 18308:2004(E) CNS	Suportar registro de dados a partir de vocabulários padrão, preservando a informação do vocabulário de origem	M	M	M
ESTR.09.R4	Ambiguidade	ISO STR4.4 TS 18308:2004(E)	Suportar regras explícitas para evitar ambigüidades quando o dado não for registrado de apenas uma maneira ou lugar. (por exemplo: explicitar o que [não] [pulso pedioso ausente] significa)	R	R	R
ESTR.09.05	Mapeamentos	ISO STR4.5 TS 18308:2004(E)	Suportar os mapeamentos entre modelos de informação e de inferência com base em um conjunto de conceitos bem definidos num vocabulário de referência ou modelo conceitual	R	R	R

ESTR.10 - Representação de texto

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
RESTR.10.01	Texto original	ISO STR 4.6 TS 18308:2004(E)	Preservar o texto original conforme fornecido pelo profissional de saúde no RES, quando a informação for traduzida da linguagem natural para outra, ou quando os termos forem mapeados de um sistema de codificação/classificação para outro	R	R	R

5.8. Requisitos de Funcionalidades

FUNC.01 - Suporte aos processos clínicos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.01.01	Evento clínico	ISO PRO1.1 TS 18308:2004(E)	Capacidade de registrar qualquer tipo de evento clínico, encontro ou episódio relevante à assistência à saúde do paciente	M	R	R
FUNC.01.02	Processos clínicos de apoio	ISO PRO1.2 TS 18308:2004(E)	Suportar a criação, acompanhamento e manutenção dos processos clínicos que apóiam as atividades de seus usuários	M	R	R
FUNC.01.03	Continuidade de processos clínicos	ISO PRO1.3 TS 18308:2004(E)	Suportar a continuidade do processo clínico, e à habilidade de se consultar o status de um processo, de se modificar um processo já existente e de se verificar se um processo foi completado	M	R	R
FUNC.01.04	Processos clínicos incompletos	ISO PRO1.4 TS 18308:2004(E)	Acomodar a existência de processos clínicos em aberto / incompletos (solicitação de exames nunca realizados)	M	R	R

FUNC.02 - Problemas / condições de saúde e outras questões

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.02.02	Condição holística do paciente	ISO PRO1.5 TS 18308:2004(E)	Registrar a condição holística da situação da saúde do indivíduo, situação funcional, problemas, condições, circunstâncias ambientais e outras questões que possam afetar a sua saúde	M	R	R
FUNC.02.02	Estrutura de dados orientada por problemas	ISO PRO1.6 TS 18308:2004(E)	Registrar e apresentar os dados em estrutura orientada por problemas incluindo o status dos problemas, planos de solução e metas. Possibilitar também estruturas como as orientadas cronologicamente, por episódios, e por processos	M	R	R
FUNC.02.03	Período de vida do paciente	ISO PRO1.7 TS 18308:2004(E)	Suportar todo o período de vida do paciente, com registro longitudinal da condição de saúde e intervenções, que devem ser visualizadas de forma cronológica. O RES é simultaneamente: retrospectivo: oferece visão histórica das condições de saúde e intervenções (ex: eventos ou atos em saúde realizados); atual: visão condição atual de saúde e intervenções ativas ou em andamento ; e prospectivo: planejamento das ações futuras (eventos ou atos em saúde pendentes ou agendados)	M	R	R

FUNC.03 - Raciocínio Clínico

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.03.01	Raciocínio clínico	ISO PRO1.8 TS 18308:2004(E)	Suportar o registro do raciocínio clínico para todos os diagnósticos, conclusões e ações a respeito da assistência à saúde do paciente, incluindo aqueles realizados por processos automatizados.	M	R	R

FUNC.04 - Suporte à decisão, protocolos clínicos e alertas.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.04.01	Alertas e lembretes	ISO PRO1.9 TS 18308:2004(E)	Suportar a apresentação automática de alertas, lembretes e avisos tais como: alergias, resultados urgentes, condição de infecção, precauções terapêuticas, intervenções importantes, e resultados urgentes	R	R	R
FUNC.04.02	Alertas e lembretes em vigilância	ISO PRO1.10 TS 18308:2004(E)	Incorporar lembretes e chamadas sobre os programas de vigilância epidemiológica e outras ações de saúde pública tais como programas de imunização ou outras campanhas.	R	R	R
FUNC.04.03	Notificação de agravos	SUS	Incorporar a notificação de agravos conforme prevê o gestor federal, estadual e municipal de saúde.	M	R	R
FUNC.04.04	Diretrizes e protocolos	ISO PRO1.11 TS 18308:2004(E)	Suportar a incorporação de diretrizes, protocolos e sistemas de apoio à decisão	R	R	R
FUNC.04.05	Restrição e obrigatoriedade	ISO PRO1.12 TS 18308:2004(E)	Suportar a representação de restrições e dados obrigatórios ao processo de apoio à decisão. Por ex., restrições de sexo X diagnóstico ou medicação X diagnóstico	R	R	R

FUNC.05 - Planejamento Terapêutico

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.05.01	Planejamento terapêutico	ISO PRO1.13 TS 18308:2004(E)	Incorporar o planejamento terapêutico incluindo gerenciamento da situação dos diferentes processos (ex: solicitado, agendado, em realização, suspenso, em pendência, complete, verificado, cancelado, complementado)	M	R	R

FUNC.06 - Prescrição e processamento de exames

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.06.01	Registro e acompanhamento	ISO PRO1.14 TS 18308:2004(E)	Suportar o registro e o acompanhamento de todas as prescrições médicas e de outros profissionais, solicitação de exames e encaminhamentos	M	R	R
FUNC.06.02	Associação	ISO PRO1.15 TS 18308:2004(E)	Associar o procedimento solicitado com o realizado e respectivo resultado	M	R	R

FUNC.07 - Assistência integral

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.07.01	Assistência integral	ISO PRO1.16 TS 18308:2004(E)	Suportar o processo de assistência integral incluindo cuidados multidisciplinares e em diferentes níveis de atenção em saúde: primário, especializado, internação hospitalar, cuidados e hospitalização domiciliar, urgência / emergência	R	R	R

FUNC.08 - Garantia de qualidade

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.08.01	Performance clínica e operacional	ISO PRO1.17 TS 18308:2004(E)	Suportar registro e consulta de dados com medidas (indicadores) de performance clínica e operacional, aderentes aos padrões de assistência com o objetivo de garantir a qualidade e medir os resultados dos processos em saúde	R	R	R

FUNC.09 - Captura de dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.09.01	Entrada e acréscimo de dados	ISO PRO2.1 TS 18308:2004(E)	Ter regras claras de consistência para entrada e acréscimos de dados, bem como para a transmissão, recebimento, tradução, substituição de dados obsoletos. Este requisito não implica em exclusão de registros. As regras locais de exclusão prevalecerão	M	M	M
FUNC.09.02	Validação de dados	ISO PRO2.2 TS 18308:2004(E)	Implementar regras de validação dos dados	M	M	M
FUNC.09.03	Pesquisa com filtros	ISO PRO2.3 TS 18308:2004(E)	Suportar a habilidade de rever informações de todos os tipos registradas no passado, inclusive via o uso de pesquisas com filtros durante o processo de captura	M	M	M

FUNC.10 - Recuperação/ consultas e visões

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.10.01	Visões	ISO PRO2.4 TS 18308:2004(E)	Suportar visões diferenciadas e recuperação seletiva para a mesma informação de para atender demandas específicas (apoio à decisão, análise de dados)	M	M	M

FUNC.11 - Apresentação dos dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.11.01	Sumário clínico	ISO PRO2.5 TS 18308:2004(E)	Ter capacidade de apresentar os dados marcados como sumário clínico de forma automática, sem a necessidade de pesquisa manual	M	M	M
FUNC.11.02	Resolução para interpretação clínica	ISO PRO2.6 TS 18308:2004(E)	Utilizar o dispositivo adequado para exibir a informação, garantindo a resolução necessária para a interpretação clínica (p.ex., imagens coloridas não devem ser exibidas em monitores monocromáticos ou visualizar uma imagem diagnóstica num monitor de baixa resolução)	M	M	M

FUNC.12 - Escalabilidade e performance

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.12.01	Eficiência de processamento	ISO PRO2.5 TS 18308:2004(E)	Processar eficientemente mesmo quando lidando com registros numerosos e/ou grandes.	R	R	R

FUNC.13 - Protocolos de mensagens

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.13.01	Exportação e importação de dados	ISO COM2.1 TS 18308:2004(E)	Suportar a exportação e a importação de dados recebidos por meio de protocolos de mensagens tais como HL7, UN/EDIFACT e DICOM	R	R	R

FUNC.14 - Troca de registros

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.14.01	Serialização	ISO COM2.2 TS 18308:2004(E)	Suportar a serialização de dados com propósito de interoperabilidade (ex: via XML, SOAP, CORBA, .Net, etc.)	R	R	R
FUNC.14.02	Regras de troca	ISO COM2.5 TS 18308:2004(E)	Prover regras de troca que sejam as mesmas para apenas um extrato do registro ou o registro completo	R	R	R
FUNC.14.03	Interoperabilidade de semântica	ISO COM2.6 TS 18308:2004(E)	Suportar interoperabilidade semântica de conceitos clínicos entre sistemas objetivando processamento automático dos dados no S-RES receptor	R	R	R

FUNC.16 - Consentimento

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.16.01	Consentimento informado	ISO PRS2.1 TS 18308:2004(E)	Suportar o registro de consentimento informado	M	M	M
FUNC.16.02	Situação do consentimento informado	ISO PRS2.2 TS 18308:2004(E)	Suportar a obtenção, registro e acompanhamento da situação do consentimento informado para acessar parte ou o todo do RES, para propósitos previamente definidos	M	M	M
FUNC.16.03	Propósito do consentimento informado	ISO PRS2.3 TS 18308:2004(E)	Suportar o registro dos propósitos pelos quais o consentimento foi obtido	M	M	M
FUNC.16.04	Instante do consentimento informado	ISO PRS2.4 TS 18308:2004(E)	Suportar o registro do instante de cada consentimento	M	M	M

FUNC.17 - Médico-legal

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.17.01	Cronologia de eventos	ISO MEL1.1 TS 18308:2004(E)	Suportar medidas que assegurem um acurado reflexo da cronologia dos eventos clínicos e das informações disponíveis no RES	M	M	M
FUNC.17.02	Precisão de visão cronológica	ISO MEL1.2 TS 18308:2004(E)	Suportar visão da representação precisa e acurada do RES de qualquer data ou hora desde a sua criação	M	M	M

FUNC.18 - Atores

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.18.01	Cuidado de uma ou mais pessoas	ISO MEL2.1 TS 18308:2004(E)	Suportar que sujeito do cuidado do RES pode ser uma ou mais pessoas	M	M	M
FUNC.18.02	Atributos clínicos relevantes	ISO MEL2.2 TS 18308:2004(E)	Suportar o registro dos atributos apropriados para a identificação do paciente e de atributos clínicos relevantes tais como data de nascimento, sexo, etnia, etc.	M	M	M
FUNC.18.03	Identificação de fornecedor de informação	ISO MEL2.3 TS 18308:2004(E)	Assegurar que usuários que atestam ou afirmam uma informação em particular no RES sejam distinta e confiavelmente identificados	M	M	M
FUNC.18.04	Identificação de usuário	ISO MEL2.4 TS 18308:2004(E)	Suportar a identificação de usuário, mesmo que este mude seu nome, profissão, sexo ou endereço	M	M	M
FUNC.18.05	Identificação dos clínicos	ISO MEL2.5 TS 18308:2004(E)	Suportar medidas que assegurem que todos os clínicos referidos em um RES sejam distintamente identificados	M	M	M
FUNC.18.06	Registro do papel dos clínicos	ISO MEL2.6 TS 18308:2004(E)	Suportar o registro do papel de qualquer clínico responsável por qualquer atividade clínica registrada no RES	M	M	M
FUNC.18.07	Datação de registro	ISO MEL2.7 TS 18308:2004(E)	Suportar medidas que assegurem que todo registro seja datada e seu autor responsável identificado	M	M	M
FUNC.18.08	Identificação de responsável de contribuição aos registros	ISO MEL2.8 TS 18308:2004(E)	Suportar medidas que assegurem que haja uma necessidade absoluta para cada contribuição nos registros seja atribuída a um ator responsável, independentemente se este atuou ou não como ator no evento	M	M	M
FUNC.18.09	Responsabilidade sobre contribuição aos registros	ISO MEL2.9 TS 18308:2004(E)	Suportar medidas que assegurem que toda contribuição aos registros seja atestada pela pessoa responsável	M	M	M

FUNC.18.10	Responsabilidade de sobre emendas e alterações de registros	ISO MEL2.10 TS 18308:2004(E)	Suportar medidas que assegurem que emendas / alterações sejam atribuídas à pessoa responsável, e que a hora/data e a razão para a emenda/alteração sejam registradas	M	M	M
------------	---	---------------------------------	--	---	---	---

FUNC.19 - Competência e governança clínica

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.19.01	Competência técnica e responsabilidade e clínica	ISO MEL3.1 TS 18308:2004(E)	Suportar a demonstração de competência clínica e responsabilidade técnica dos clínicos	R	R	R

FUNC.20 – Fé Pública

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.20.01	Substituição de dados	ISO MEL4.1 TS 18308:2004(E)	Assegurar que as novas informações entradas, para substituição de outras previamente registradas, sejam coletadas separadamente e atestadas como em substituição àquelas previamente registradas	M	M	M
FUNC.20.02	Situação de registro	ISO MEL4.2 TS 18308:2004(E)	Assegurar que a exata situação do registro possa ser recriada em um dado ponto no tempo desde a criação original do RES	M	M	M

FUNC.21 - Preservação de contexto

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.21.01	Preservação da linguagem original do registro	ISO MEL5.1 TS 18308:2004(E)	Suportar que textos ou rubricas originais sejam preservados na linguagem original, onde o texto ou termos codificados no RES tenham sido traduzidos ou mapeados	R	R	R
FUNC.21.02	Associação da informação do contexto clínico	ISO MEL5.2 TS 18308:2004(E)	Manter a associação da informação do contexto clínico e elementos de dados relevantes independentemente de como os dados foram estruturados	M	M	M

FUNC.22 - Permanência

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.22.01	Permanência	ISO MEL6.1 TS 18308:2004(E)	Assegurar que a informação atestada seja armazenada em modo protegido de tal sorte a impedir qualquer alteração ou exclusão	M	M	M

FUNC.23 - Controle de versão

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.23.01	Controle de versões	ISO MEL7.1 TS 18308:2004(E)	Suportar controle de versões de acordo com a granularidade que a informação foi atestada	M	R	R
FUNC.23.02	Medidas de discernimento	ISO MEL7.2 TS 18308:2004(E)	Suportar medidas de discernimento de modificação ou atualização do registro usando controle de versão	M	M	M

FUNC.24 - Ética

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.24.01	Registro de justificativa ética	ISO ETH1.1 TS 18308:2004(E)	Suportar o registro da justificativa ética e da aprovação para uso secundário da informação do paciente constante no RES	M	M	M

FUNC.25 - Direitos do consumidor

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.25.01	Visão orientada para o consumidor	ISO COC1.1 TS 18308:2004(E)	Suportar uma visão do RES orientada para o consumidor	R	R	R
FUNC.25.02	Direito de acesso	ISO COC1.2 TS 18308:2004(E)	Suportar o direito de acesso a todas as informações do RES sujeitas a questões legais	M	M	M
FUNC.25.03	Informações dos consumidores	ISO COC1.3 TS 18308:2004(E)	Suportar a incorporação no RES de informações dos consumidores sobre autocuidado, ponto de vista pessoal sobre as questões de saúde, níveis de satisfação, expectativas e comentários, quando manifestarem desejo	M	R	R

FUNC.26 - Questões culturais

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.26.01	Interoperabilidade de	ISO COC2.1 TS 18308:2004(E)	Suportar a interoperabilidade de tal sorte que seja realmente global, respeitando, contudo, os costumes e cultura locais. O processo deve ser sempre simples e adaptável a diferentes ambientes legais	R	R	R

FUNC.27 - Evolução

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	A	S	G
FUNC.27.01	Compatibilidade e com arquiteturas e versões antigas	ISO EVO1.1 TS 18308:2004(E)	Ser compatível com arquiteturas e versões antigas dos S-RES, de tal sorte que possa processar dados criados nessas versões.	O	O	O
FUNC.27.02	Compatibilidade e com arquiteturas e versões mais novas	ISO EVO1.2 TS 18308:2004(E)	Ser compatível com arquiteturas e versões mais novas dos S-RES, de tal sorte que possa processar dados criados nessas versões.	M	M	M
FUNC.27.03	Novos conhecimentos	ISO EVO1.3 TS 18308:2004(E)	Ser capaz de acomodar o registro de informação relacionada a novos conhecimentos clínicos, novas disciplinas clínicas, e novas práticas e processos clínicos.	R	R	R

5.9. Requisitos TISS

O conjunto de requisitos abaixo descritos verifica se os sistemas de informação de prestadores de serviços de saúde (grupos 1, 2 e 3) e de operadoras de planos de saúde (médico e/ou odontológicos) atendem os requisitos de conteúdo e estrutura do padrão TISS. A definição dos sistemas que se enquadram em cada grupo pode ser consultada na Tabela 2, na seção 5.3.

TISS.01 – Conteúdo e Estrutura para Prestadores do Grupo 1

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Grupo 1*	SADT Isolados
TISS.01.01	Guia de Consulta TISS	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar e/ou gerar os dados da Guia de Consulta TISS, conforme: http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/consulta/Guia_Consulta.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X
TISS.01.02	Guia de Serviços Profissionais / SADT	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar e/ou gerar os dados da Guia de Serviços Profissionais / Serviço Auxiliar Diagnóstico e Terapia (SP/SADT) TISS, conforme http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/sp-sadt/Guia_SADT.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X
TISS.01.03	Guia TISS de Solicitação de Internação	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de Solicitação de Internação, conforme http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/solicita%20interna%E7%E3o/Guia_Solicitacao_Internacao.xls e gerar este conteúdo em XML para compor a mensagem eletrônica “SOLICITACAO_PROCEDIMENTOS” conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X

* Grupo 1 – inclui todos os S-RES no Grupo 1 da Tabela 2 (seção 5.3), EXCETO S-RES para SADT isolados.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Grupo 1*	SADT Isolados
TISS.01.04	Guia TISS de Resumo de Internação	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de Resumo de Internação, conforme http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/resumo%20e%20interna%E7%E3o/Guia_Resumo_Internacao.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X
TISS.01.05	Guia TISS de Honorário Individual	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de e Honorário Individual conforme http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/Honor%E1rio%20Individual/Guia_Honorario_Individual.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	R
TISS.01.06	Guia TISS de Outras Despesas	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de Outras Despesas conforme http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/outras%20despesas/Guia_Outras_Despesas.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	O	R

* Grupo 1 – inclui todos os S-RES no Grupo 1 da Tabela 2 (seção 5.3), EXCETO S-RES para SADT isolados.

TISS.02 – Conteúdo e Estrutura para Prestadores do Grupo 2

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.02.01	Guia de Consulta TISS	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 2 deve ser capaz de capturar e/ou gerar os dados da Guia de Consulta TISS , conforme: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/consulta/Guia_Consulta.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.02.02	Guia TISS de Solicitação de Internação	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 2 deve ser capaz de capturar os dados da Guia TISS de Solicitação de Internação , conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/solicita%20interna%E7%E3o/Guia_Solicitacao_Internacao.xls e gerar este conteúdo em XML para compor a mensagem eletrônica “SOLICITACAO_PROCEDIMENTOS” conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.02.03	Guia de Serviços Profissionais / SADT	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 2 deve ser capaz de capturar e/ou gerar os dados da Guia de Serviços Profissionais / Serviço Auxiliar Diagnóstico e Terapia (SP/SADT) TISS , conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/sp-sadt/Guia_SADT.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M

TISS.03 – Conteúdo e Estrutura para Prestadores do Grupo 3

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.03.01	Guia de Tratamento Odontológico - Solicitação	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 3 deve ser capaz de capturar os dados da Guia TISS de Tratamento Odontológico - Solicitação conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/tratamento%20odontol%F3gico/Guia_Solicitacao_odontologia.xls e gerar este conteúdo em XML para compor a mensagem eletrônica AUTORIZACAO_ODONTOLOGIA conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M

TISS.03.02	Guia de Tratamento Odontológico - Cobrança	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 3 deve ser capaz de capturar os dados da Guia TISS de Tratamento Odontológico - Cobrança conforme http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/tratamento%20odontol%F3gico/Guia_Cobranca_odontologia.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M
------------	--	--------------------------	--	---

TISS.04 – Conteúdo e Estrutura para Operadoras de Planos de Assistência Médica

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.04.01	Demonstrativo de Pagamento	ANS – RN 153, 29/05/2007	O sistema de informações das operadoras de planos de assistência medica deverá gerar os dados do Demonstrativo de Pagamento , conforme: http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/demonstrativos/Demonstrativo.doc	M
TISS.04.02	Demonstrativo de Análise de Conta Médica	ANS – RN 153, 29/05/2007	O sistema de informações das operadoras de planos de assistência medica deverá gerar os dados do Demonstrativo de Análise de Conta Médica http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/demonstrativos/Demonstrativo Conta Medica.doc	M

TISS.05 – Conteúdo e Estrutura para Operadoras exclusivamente de Planos Odontológicos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.05.01	Guia de Tratamento Odontológico - Demonstrativo de Pagamento	ANS – RN 153, 29/05/2007	O sistema de informações das operadoras de planos exclusivamente odontológicos deverá gerar os dados do Guia de Tratamento Odontológico - Demonstrativo de Pagamento , conforme: http://www.ans.gov.br/portal/site/hotsite_tiss/pdf/guias/tratamento_odontol%F3gico/Guia_demonstrativo_pagamento_Odonto.xls	M

TISS.06 – Comunicação para prestadores das categorias 1 e 2

A tabela abaixo descreve o conjunto de requisitos de comunicação para que os sistemas de informação de prestadores dos grupos 1 e 2 (ver seção 5.3) estejam aptos a enviar e receber todas as mensagens XML previstas no padrão TISS, conforme prevêem a RN 153 de 29/05/2007 e a IN nº 26, de 10/05/2007. Observar que o conteúdo das mensagens em XML deve obedecer aos esquemas descritos acima nos requisitos de conteúdo, de acordo com o grupo no qual o S-RES se enquadra, conforme classificação da ANS. Por exemplo, em se tratando de S-RES de consultório médico este deverá enviar as Guias de Faturamento de seu contexto, ou seja, as Guias de Consulta. Portanto, não será exigido que um S-RES de consultório seja capaz de enviar Guias de Resumo de Internação.

Conforme o Manual de Comunicação e Segurança das Mensagens TISS, a comunicação prestador operadora poderá ser: via WebServices (preferencialmente), via troca de arquivos em diretórios de entrada e saída, também definidos pelo padrão TISS, ou, ainda através de “upload” no site das operadoras. Cada uma das mensagens abaixo descritas deverá, portanto, obedecer a pelo menos um destes métodos de comunicação para que o S-RES nesta categoria venha a ser certificado.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.06.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS : ENVIO_GUIAS conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.06	Protocolo de Recebimento Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS “PROTOCOLO_RECEBIMENTO” conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.04	Recebimento da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.05	Solicitação de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS SOLICITACAO_PROCEDIMENTOS , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.06	Recebimento Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.06.08	Solicitação dos Demonstrativos de Retorno	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLIC_DEMONTISS.04.07STRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.09	Recebimentos demonstrativos de pagamento, da análise de contas médicas e de odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber as mensagens TISS DEMONSTRATIVO_PAGAMENTO" "DEMONSTRATIVO_ANALISE_CONTA_MEDICA" "DEMONSTRATIVO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.10	Re-apresentação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.06.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O
TISS.06.13	Recebimento da resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O

TISS.07 – Comunicação para prestadores da categoria 3

A tabela abaixo descreve o conjunto de requisitos de comunicação para que os sistemas de informação de prestadores do grupo 3 estejam aptos a enviar e receber todas as mensagens XML previstas no padrão TISS, conforme prevêem a RN 153 de 29/05/2007 e a IN nº 26, de 10/05/2007 2007.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.07.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS : ENVIO_GUIAS conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.07	Protocolo de Recebimento do Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS “PROTOCOLO_RECEBIMENTO” conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.04	Recebimento da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.05	Solicitação de Autorização Procedimentos Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS AUTORIZACAO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.07	Recebimento da Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.08	Solicitação dos Demonstrativos de Retorno Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLIC_DEMONSTRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.09	Recebimento, Demonstrativo de Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber as mensagens TISS " "DEMONSTRATIVO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.07.10	Re-apresentação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.07.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O
TISS.07.13	Recebimento da resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O

TISS.08 – Comunicação para Operadoras de Planos de Assistência Médica

A tabela abaixo descreve o conjunto de requisitos de comunicação para que os sistemas de informação de operadoras de planos de assistência médica estejam aptos a enviar e receber todas as mensagens XML previstas no padrão TISS, conforme prevêem a RN 153 de 29/05/2007 e a IN nº 26, de 10/05/2007 2007.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.08.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS : ENVIO_GUIAS conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.08	Protocolo de Recebimento do Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar às operadoras a mensagem TISS “PROTOCOLO_RECEBIMENTO” conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.04	Envio da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.05	Solicitação de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a Mensagem TISS SOLICITACAO_PROCEDIMENTOS , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.08.08	Envio da Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz enviar aos prestadores a mensagem TISS AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.08	Solicitação dos Demonstrativos de Retorno	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLIC_DEMONTISS.04.07STRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.09	Envio Demon. Pagamento, e da Análise de contas Médicas	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores as mensagens TISS DEMONSTRATIVO_PAGAMENTO" "DEMONSTRATIVO_ANALISE_CONTA_MEDICA", conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.10	Re-apresentação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.08.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O
TISS.08.13	Resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O

TISS.09 – Comunicação para Operadoras exclusivamente de Planos Odontológicos

A tabela abaixo descreve o conjunto de requisitos de comunicação para que os sistemas de informação de operadoras exclusivamente de planos odontológicos estejam aptos a enviar e receber todas as mensagens XML previstas no padrão TISS, conforme prevêem a RN 153 de 29/05/2007 e a IN nº 26, de 10/05/2007 2007.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESEÇA
TISS.09.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS : ENVIO_GUIAS conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.09	Protocolo de Recebimento do Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem TISS “PROTOCOLO_RECEBIMENTO” conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em: http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.04	Envio da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.05	Solicitação de Procedimentos Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a Mensagem TISS AUTORIZACAO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.09	Envio da Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz enviar aos prestadores a mensagem TISS AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.09	Solicitação dos Demonstrativos de Retorno	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLIC_DEMONTISS.04.07STRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.09	Envio Demon. de Pagamento, e da Análise de contas Médicas	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores as mensagens TISS DEMONSTRATIVO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.10	Re-apresentação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.09.12	Verificação de	ANS – RN 153,	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS	O

	Elegibilidade	29/05/2007 e IN nº 26, de 10/05/2007	VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	
TISS.09.13	Envio da resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/esquemas	O

6. Referências

- [1] CFM. Resolução 1638/2002. On-line. Disponível em: http://www.portalmédico.org.br/resolucoes/cfm/2002/1638_2002.htm
- [2] CFM. Resolução 1639/2002.. On-line. Disponível em: http://www.portalmédico.org.br/resolucoes/cfm/2002/1639_2002.htm
- [3] MEDIDA PROVISÓRIA No 2.200-2, DE 24 DE AGOSTO DE 2001. On-line. Disponível em: https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm
- [4] Cadastro Nacional de Usuários do Sistema Único de Saúde. Disponível em: <http://cartaonet.datasus.gov.br/>
- [5] Cadastro Nacional de Estabelecimentos e Profissionais de Saúde – CNES. Disponível em: <http://www.datasus.gov.br/cnes>
- [6] Padrão TISS. Disponível em: http://www.ans.gov.br/portal/site/hotsite_tiss
- [7] ISO/TR 20.514:2005 Technical Report - Health informatics -- Electronic health record -- Definition, scope and context. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39525
- [8] ISO/TS 18.308:2004 - Health informatics -- Requirements for an electronic health record architecture. Disponível em: <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33397>
- [9] HL7 – Health Level 7 – <http://www.hl7.org>
- [10] HL7 -EHR Functional Model. Disponível on line: <http://www.hl7.org/EHR/>
- [11] CCHIT. Commercial Certification Handbook. Ambulatory EHR Products. Disponível em: http://www.cchit.org/files/Ambulatory_Domain/2007AEHRCertificationHandbookV2_1.pdf
- [12] ISO/FDIS - 21549-7 - Health informatics - Patient healthcard data - Part 7: Medication data - Final draft 2007
- [13] Mon, Donald T.. “Difference Between the EHR Standard and Certification.” Journal of AHIMA 77, no.5 (May 2006): 66,68,70.
- [14] ISO/IEC 27.002:2005 - Information technology -- Security techniques -- Code of practice for information security management. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297
- [15] ABNT NBR ISO/IEC 27.002:2005 (antiga NBR ISO/IEC 17799:2005) - Código de Prática para a Gestão da Segurança da Informação. Disponível em: <http://www.abntnet.com.br/ecommerce/default.aspx>

- [16] [ISO/IEC 15.408-1:2005](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612) Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612
- [17] [ISO/IEC 15.408-2:2005](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40613) Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40613
- [18] [ISO/IEC FCD 15.408-3:2005](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40614) Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40614
- [19] ABNT NBR ISO/IEC 27.001:2006 Sistemas de Gestão de Segurança da Informação – Requisitos. Disponível em: <http://www.abntnet.com.br/ecommerce/default.aspx>
- [20] ETSI TS 101 733: ETSI. "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".