Ata da 50ª Reunião Ordinária do Grupo Coordenador do COPISS – Comitê de Padronização das Informações em Saúde Suplementar.

Às 14 horas do dia nove de fevereiro de dois mil e doze, nesta cidade, à Rua Teixeira de Freitas, nº 05 – 2º andar, realizou-se a 50ª reunião ordinária do COPISS – Comitê de Padronização das Informações em Saúde Suplementar. A reunião foi coordenada por Antonio Carlos Endrigo, Gerente Geral de Integração Setorial e contou com a presença de 14 das 22 instituições componentes do COPISS. Como titulares participaram: Anísio Rodriguez Neto (Unimed), Antonio Carlos Endrigo (ANS), Eduardo de Oliveira (FBH), Erimar Carlos Brehme de Abreu (CMB), Florisval Meinão (AMB), José Alves de Souza Neto (Uniodonto), Luiz Antônio de Biase (ABRAMGE), Marizélia Leão Moreira (ANS), Murilo Alves Moreira (ANAHP), Paulo R. Azevedo (SBPC/ML). Como suplentes participaram: Carlos Eduardo Moura (CBR), Cláudia Durante (SINOG), Ericson Leão Bezerra (CFO), João de Lucena Gonçalves (CNS). Na condição de ouvintes participaram: Cristina Gama Dias (FBH), Danilo Valter Bernik (FEHOSP/SINDHOSP), João Alfredo Gonçalves (CMB), Gilberto Bosco Neto e Rosimeri I. Lima (FENASAÚDE), Patrícia Yazbel e Rodrigo Alves da Silva (Orizon), Sílvio P. Sanches (SINOG) e Wilson Shcolnik (SBPC/ML). Não estiveram representadas na reunião: ANVISA; CFM; DIPRO/ANS, FENAM e UNIDAS. Não têm representantes indicados até a presente data as Instituições Públicas de Ensino e Pesquisa, a representação dos beneficiários e o DATASUS/MS. Como representante de entidades convidadas esteve presente o Sr. Luis Kiatake (SBIS) e ausente a SAS/MS. A reunião foi acompanhada por Bruno de Paula Soares, Celina Maria Ferro de Oliveira, Jorge Luizi Pinho, Júlio César di Maio, Marluce Chrispim e Teófilo Rodrigues, da Gerência de Padronização e Interoperabilidade da ANS. O coordenador deu início aos trabalhos com o propósito de apreciar a pauta prevista para a reunião, tratando dos seguintes assuntos: **a)** leitura, aprovação e assinatura da ata da reunião anterior – 49ª reunião do COPISS coordenador; **b)** informado sobre a organização, pelo CFM, de seminário para debater o tema "sigilo e confidencialidade dos dados de saúde", com previsão para o dia 17/04/2012; **c)** informado sobre a solicitação feita à SBIS para que haja a prorrogacão do prazo de disponibilidade da consulta pública referente ao Manual de Certificação para Sistemas de Registro Eletrônico em Saúde até 15/02/2012; **d)** Informado sobre a elaboração do Relatório de atividades do COPISS em 2011, seguindo a estrutura proposta na reunião do COPISS de fevereiro de 2011 e acordado o envio de material complementar pelos membros do COPISS até 24/02/2012 e disponibilização da versão preliminar em 29/02/2012; **e)** informado a atualização da relação de coordenadores TISS no

ambiente colaborativo do COPISS e representação à Diretoria de Fiscalização das operadoras que não atenderam a notificação, pelo descumprimento da RN 190; **f)** apresentada a análise inicial do Radar TISS, edição de 2011. Para a pesquisa foram selecionadas 1.242 operadoras, das quais 86% enviaram todos os dados solicitados; **g)** apresentado pela Coordenadora Celina Oliveira algumas questões do componente de Conteúdo e Estrutura decorrentes da análise efetuada pelo COPISS do material entregue em 15/12/2011. O resultado da apreciação do COPISS sobre o tema encontra-se registrado na Nota desta reunião; **h)** informada a disponibilização no ambiente colaborativo do COPISS de nova versão das terminologias de Procedimentos e eventos em saúde e de Diárias, taxas e gases medicinais com as atualizações decorrentes da análise da Consulta Pública para apreciação dos respectivos grupos de trabalho. Solicitado que as observações sobre possíveis inconsistências em relação ao material apresentado sejam encaminhadas à GERPI/GGISE até o dia 02/03/2012; **i)** apresentado por João Paulo Pereira de Souza, procurador da PROGE/ANS, resposta ao questionamento da FENASAÚDE ao GT de Segurança e Privacidade acerca da validade jurídica dos documentos em meio eletrônico, cujo conteúdo encontra-se transcrito parcialmente na Nota COPISS desta reunião. O COPISS considerou que a resposta atende à demanda de todas as operadoras e foi acordado que a questão deve integrar o conjunto de perguntas e respostas do Padrão TISS; **j)** apresentado um resumo com as principais proposições da reunião do GT Segurança e Privacidade, ocorrida em 09/02/2012 das 9h00 às 12h00, com destaque para o documento de requisitos deste componente e outras relativas ao caráter condicional de algumas mensagens eletrônicas. O resultado da apreciação do COPISS encontra-se registrado na Nota desta reunião; **k)** acordada a próxima reunião do COPISS Coordenador para o dia 29/03/2012. O Coordenador do COPISS considerou cumprida a pauta, dando por encerrada a presente reunião.

Rio de Janeiro, 09 de fevereiro de 2012.

Antonio Carlos Endrigo	Anísio Rodriguez Neto
ANS	UNIMED

Carlos Eduardo Moura	Cláudia Durante
CBR	SINOG
Eduardo de Oliveira	Ericson Leão Bezerra
FBH	CFO
Erimar Carlos Brehme de Abreu	Florisval Meinão
CMB	AMB
José Alves de Souza Neto	João de Lucena Gonçalves
Uniodonto	CNS
Luiz Antônio de Biase	Luis Kiatake
ABRAMGE	SBIS

Marizélia Leão Moreira	Murilo Alves Moreira
ANS	ANAHP

Paulo Roffé Azevedo

SBPC

Nota da 50ª reunião ordinária do COPISS, realizada no dia 09 de fevereiro de 2012.

Assunto: Proposições para atualização do Padrão de Troca de Informação na Saúde Suplementar (Padrão TISS), decorrentes da Consulta Pública 43.

Referências: (1) consolidação das proposições sobre o componente de conteúdo e estrutura e alterações elaboradas pela Gerência de Padronização e Interoperabilidade; **(2)** questionamento da FENASAÚDE - Ofício DISAU nº 008/2012 – acerca da validade jurídica dos documentos em meio eletrônico e resposta da PROGE/ANS e **(3)** apresentação do trabalho realizado pelo GT de Comunicação e Segurança em 09/02/2012, sobre as regras de segurança e privacidade de acesso às informações do padrão TISS.

Apresentação: A presente Nota traz as proposições do COPISS quanto às questões acima referidas para o aprimoramento do Padrão TISS, sendo as seguintes:

1) Sobre o Componente de Conteúdo e Estrutura

1.1) Mensagem de retorno de recebimento de anexos:

A mensagem de retorno conterá os dados de autorização, com a indicação de preenchimento condicionado. Os dados de autorização também farão parte da mensagem de Resposta ao Status da Autorização.

1.2) Anexo de OPME:

Alteração do campo "opção do fabricante", para indicação de material.

1.3) Criação de nova mensagem para indicar a "solicitação de execução":

Criar uma mensagem para as situações em que a solicitação de SP/SADT é encaminhada por um prestador diferente do prestador executante. Isto é necessário para que a mensagem de solicitação de autorização enviada pelo executante seja entendida como um complemento da solicitação anterior e não como uma nova solicitação dos mesmos procedimentos.

1.4) Mensagem de Resumo de Internação:

Exclusão dos seguintes campos referentes a Internação Obstétrica, por avaliação da DIPRO: Informações da internação obstétrica, Qtde RN em UTI Neonatal com permanência até 48 horas, Óbito em mulher, Óbito neonatal, Qtde nascidos vivos a termo, qtde nascidos mortos, Qtde nascidos vivos prematuros.

1.5) Cabeçalho das mensagens:

O cabeçalho das mensagens eletrônicas não conterá a identificação da empresa, software e versão do software do sistema utilizado pelo prestador.

1.6) Mensagem Demonstrativo de Análise de Conta:

Não será feita a inclusão de indicador de Guia em Análise.

1.7) Obrigatoriedade das mensagens:

O Padrão TISS conterá mensagens obrigatórias, condicionadas e não obrigatórias. As mensagens não obrigatórias, quando implementadas, deverão seguir o Padrão TISS.

2) Sobre a Validade Jurídica dos Documentos em Meio Eletrônico – questionamento da FENASAÚDE através do Ofício DISAU nº 008/2012, e resposta da PROGE/ANS

Em relação ao questionamento da FENASAÚDE acerca da validade jurídica dos documentos em meio eletrônico, a Procuradoria Federal junto à ANS – PROGE/ANS, apresentou o parecer transcrito parcialmente abaixo, que o COPISS considera esclarecedor da demanda da Federação. Para melhor entendimento do texto, considera-se:

- CC – Código Civil;
- CPC – Código de Processo Civil e
- CF – Constituição Federal.

'Trata-se de ofício enviado pela FENASAÚDE – Federação Nacional de Saúde Suplementar solicitando a inclusão do tema "validade legal dos documentos trocados em meio eletrônico dos anexos das guias TISS" na pauta da reunião do GT de Comunicação e Segurança do dia 09/02/2012.

De acordo com a FENASAÚDE, as operadoras têm dúvidas sobre a "validade legal" perante as mais diversas instâncias (Judiciário, autoridades fazendárias dos entes da federação e órgãos reguladores e fiscalizadores etc) de documentos recebidos em meio magnético – poderiam eles ser utilizados como provas em ações judiciais de qualquer natureza, em autuações fiscais ou mesmo diante dos órgãos reguladores e fiscalizadores?

De início, o que foi tratado no ofício como "validade legal", permite-se corrigir para "admissibilidade e eficácia probatórias".

Com efeito, a validade jurídica é qualidade que pode ter o negócio jurídico, satisfeitos os requisitos previstos no art. 104 do CC, e não propriamente o documento que o espelha.

Dente os requisitos de validade do negócio jurídico elencados no art. 104 do CC, que valem também para os atos jurídicos por força do art. 185 do CC, está a "forma prescrita ou não defesa em lei".

Assim, quando a forma não é observada, o que deixa de ter validade jurídica é o negócio e não o documento que o consubstancia.

Posto isso, tem-se que a regra, no nosso ordenamento jurídico, é não ser exigida forma especial para a validade do ato ou do negócio.

A mesma regra vale para a sua eficácia probatória, eis que o CPC, no art. 332, estabelece claramente que "Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa".

Portanto, a eficácia probatória é um atributo que a lei confere livremente a qualquer meio legal, ainda que não especificado no CPC, ou moralmente legítimo, que seja hábil para provar a verdade dos fatos.

Conjugando o CPC com a CF (art. 5º, LVI – "são inadmissíveis, no processo, as provas obtidas por meios ilícitos"), pode-se afirmar, mais simplesmente, que não sendo ilícito, qualquer meio de prova é admitido.

Diante disso, não há qualquer restrição legal à admissibilidade, como prova, de documentos eletrônicos, desde que produzidos licitamente.

Quanto à eficácia probatória desses mesmos documentos, basta que sejam hábeis para provar a verdade do fato a que se referem.

A doutrina, nesse aspecto, estabelece quatro requisitos para que os documentos eletrônicos possam ser aceitos como meio de prova:

a) autenticidade: certeza de que o documento provém do autor nele indicado;

b) integridade: certeza de que o documento não foi alterado ou corrompido, durante o seu envio, recebimento e armazenamento; não pode o documento ser passível de alteração, ou quando o for, deve ser possível a identificação da alteração sofrida;
c) perenidade: refere-se à validade da informação ou do conteúdo do documento ao longo do tempo; na preservação de documentos digitais é necessária a adoção de ferramentas que protejam e garantam a sua manutenção; e
d) tempestividade: viabilidade de se obter com certeza a data em que o documento foi produzido ou elaborado.

Havendo recursos técnicos que ofereçam aos registros eletrônicos esses requisitos mínimos acima citados, pode-se afirmar que, em processos judiciais, não se poderá a eles negar eficácia probatória...

...Logo, para fins de eficácia probatória no plano judicial, e, por corolário, para fins de eficácia probatória geral, pode-se sugerir que o GT em comento verifique se os procedimentos adotados por força da RN 153/2007 garantem o preenchimento dos quatro requisitos mínimos aqui listados para que os registros eletrônicos tenham força probatória.

O mesmo vale para o plano administrativo, em regra, tendo em vista que a Lei de Processo Administrativo Federal, em seu art. 30, repete a CF, apenas repelindo as provas obtidas por meios ilícitos.

No entanto, admite-se que possam existir normas específicas a impor forma especial para a validade ou prova de determinado ato perante algum ente administrativo outro que não a ANS a que estejam sujeitas as operadoras.

Entretanto, tal circunstância foge à esfera regulatória da ANS.

Cabe às operadoras verificar a existência de disciplina específica por parte de algum ente administrativo a que também estejam sujeitas além da ANS e adotar as providências necessárias para respeitá-las, o que, todavia, repita-se, trata-se de matéria estranha à ANS.'

3) <u>Sobre as Regras de Segurança e Privacidade:</u>

3.1) Identificar e autenticar todo usuário antes de qualquer acesso a dados com identificação do beneficiário.

3.2) Utilizar para autenticação de usuários em site e páginas da Internet (portais) login e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital.

3.3) Utilizar para autenticação de usuários, via utilização de webservices, login e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital.

3.4) Verificar a qualidade de segurança da senha no momento de sua definição pelo usuário, obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser não alfabético.

3.5) Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento.

3.6) Armazenar a senha dos usuários utilizando qualquer algoritmo HASH.

3.7) Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de login. Este número de tentativas não deve ser superior a cinco.

3.8) Possuir controles de segurança na sessão de comunicação a fim de não permitir o roubo de sessão do usuário.

3.9) Oferecer, na sessão de comunicação entre o componente cliente e o componente servidor, os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados.

3.10) Encerrar a sessão do usuário após período de tempo configurável de inatividade. Este tempo não deve ser superior a trinta minutos.

3.11) Registrar log de acessos e de tentativas de acesso ao sistema de informação.

3.12) Utilizar certificado digital dentro do período de validade e não aceitar o certificado se o mesmo estiver na lista de certificados revogados da Autoridade Certificadora.

3.13) Utilizar certificado digital que identifique o endereço eletrônico para o qual foi emitido.

3.14) Utilizar certificado digital que contemple em sua estrutura a identificação da autoridade certificadora emissora.

3.15) Utilizar certificado digital que contemple em sua estrutura a identificação do titular do certificado.

3.16) Utilizar certificado digital que utilize protocolo criptográfico SSL ou TLS.

3.17) Utilizar certificado digital que utilize criptografia de, no mínimo, 128 bits.

3.18) Utilizar certificado digital que implemente autenticação por algoritmo HASH.

Rio de Janeiro, 09 de fevereiro de 2012.

Antonio Carlos Endrigo	Anísio Rodriguez Neto
ANS	UNIMED
Carlos Eduardo Moura	Cláudia Durante
CBR	SINOG
Eduardo de Oliveira	Ericson Leão Bezerra
FBH	CFO
Erimar Carlos Brehme de Abreu	Florisval Meinão
CMB	AMB
José Alves de Souza Neto	João de Lucena Gonçalves
Uniodonto	CNS
Luiz Antônio de Biase	Luis Kiatake
ABRAMGE	SBIS

Marizélia Leão Moreira	Murilo Alves Moreira
ANS	ANAHP

Paulo Roffé Azevedo

SBPC