CARLOS HENRIQUE JACOB

**Análise do uso de novas tecnologias na troca
e armazenamento de informações de saúde e o
segredo profissional**

São Paulo

2009

CARLOS HENRIQUE JACOB

**Análise do uso de novas tecnologias na troca
e armazenamento de informações de saúde e o
sigilo profissional**

Dissertação apresentada à Faculdade
de Odontologia da Universidade de São
Paulo para obtenção do título de Mestre
em Ciências Odontológicas.

Área de Concentração: Odontologia
Social

Orientador: Prof. Dr. Rogerio Nogueira
de Oliveira

São Paulo

2009

Catálogo-na-Publicação
Serviço de Documentação Odontológica
Faculdade de Odontologia da Universidade de São Paulo

Jacob, Carlos Henrique

Análise do uso de novas tecnologias na troca e armazenamento de informações de saúde e o sigilo profissional / Carlos Henrique Jacob; orientador Rogério Nogueira de Oliveira. -- São Paulo, 2009.

81p. : fig.; 30 cm.

Dissertação (Mestrado - Programa de Pós-Graduação em Ciências Odontológicas. Área de Concentração: Odontologia Social) -- Faculdade de Odontologia da Universidade de São Paulo.

1. Segredo profissional – Responsabilidade pela informação 2. Sistemas de informação – ANS (Brasil) – Segurança 3. Segurança em sistemas computacionais – Serviços de Saúde 4. Odontologia Social

CDD 614.1
BLACK D585

AUTORIZO A REPRODUÇÃO E DIVULGAÇÃO TOTAL OU PARCIAL DESTE TRABALHO, POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE E COMUNICADA AO AUTOR A REFERÊNCIA DA CITAÇÃO.

São Paulo, ____/____/____

Assinatura:

E-mail: ch.jacob@yahoo.com

FOLHA DE APROVAÇÃO

Jacob CH. Análise do uso de novas tecnologias na troca e armazenamento de informações de saúde e o sigilo profissional. Dissertação apresentada à Faculdade de Odontologia da Universidade de São Paulo para obtenção do título de Mestre em Ciências Odontológicas.

Aprovado em: / /

Banca Examinadora

Prof(a). Dr(a). _____ Instituição: _____

Julgamento: _____ Assinatura: _____

Prof(a). Dr(a). _____ Instituição: _____

Julgamento: _____ Assinatura: _____

Prof(a). Dr(a). _____ Instituição: _____

Julgamento: _____ Assinatura: _____

A meu pai, Edgard Jacob, cujos atos de bondade e justiça me trouxeram ao caminho reto, em um tempo de atalhos tortuosos.

A meus avós, Francisco Lopes dos Santos e Hugo Jacob, cujas ausências me inspiraram mais a respeito do sentido da vida que qualquer conversa, qualquer livro, excedendo qualquer sombra de dúvida. Porque a verdade, em verdade, só é transmitida de coração a coração. Palavras atrapalham.

AGRADECIMENTOS

Nenhum trabalho é feito por um só homem. É, todavia, impossível fazer uma lista de todas as pessoas que para contribuíram. Seguem, abaixo descritas, as pessoas cuja contribuição foi mais relevante, sem as quais partes essenciais deste quebra cabeça-jamais teriam sido juntadas.

Ao professor Dr. Rogerio Nogueira de Oliveira, pela confiança e disponibilidade na orientação deste trabalho.

À professora Dra. Ida Tecla Prellwitz Calvielli, pela convivência, amizade, generosidade.

Ao professor Dr. Rodolfo Melani, exemplo de retidão em tempos perigosos.

Aos professores do Departamento de Odontologia Social da Faculdade de Odontologia da Universidade de São Paulo, pela acolhida e disponibilidade.

À professora Dra. Mary Caroline Skelton-Macedo, pela amizade, confiança e apoio.

Aos funcionários da Biblioteca da Faculdade de Odontologia da Universidade de São Paulo, em especial à bibliotecária Maria Cláudia Pestana, pela adequação das Referências às normas vigentes.

À amiga Tatiana Toporcov, conspiradora.

À colega e amiga Mariana Trigueiro, que não desiste.

Aos amigos Theo, Lilian, Marcos, Vanessa, Frederico e Thais, porque estavam lá.

Ao Ricardo e ao Scooby, pela atenção e disponibilidade na correção do vernáculo.

A meus eternos irmãos em espírito, Caio, Deco, Felipe, Kulik e Rolhão; Alessandra, Andréa e Maria Rita, pelas noites estreladas de esperança, porque sabem que, na verdade, não há luta vã.

À mais que amiga Fernanda Martinazzo, pelo necessário caos criativo, pela paciência e incentivo constantes.

A meus inimigos, que me tornaram melhor do que sou.

À tríade irresistível: minha irmã, minha avó, minha mãe.

Roma locuta, causa finita.
(máxima latina)

Auctoritas siquidem ex vera ratione processit, ratio vero
nequaquam ex auctoritate.
— Iohannes Scottus, *De Divisione Naturae*

Die stillsten Worte sind es, welche den Sturm bringen.
Gedanken, die mit Taubenfüßen kommen, lenken die
Welt.
— Friedrich Nietzsche

RESUMO

Jacob CH. Análise do uso de novas tecnologias na troca e armazenamento de informações de saúde e o sigilo profissional [dissertação]. São Paulo: Universidade de São Paulo, Faculdade de Odontologia; 2009.

O caráter privativo das informações de saúde, reconhecido e valorizado desde a antigüidade clássica, hoje é considerado como um dos fatores indispensáveis à manutenção da sociedade, das garantias constitucionais de liberdade e também, em última instância, à própria democracia. Essa importância é demonstrada pela existência do segredo profissional, que, para as profissões da área da saúde (como medicina, odontologia, psicologia, nutrição etc.) de um modo positivo, coloca aos profissionais a necessidade de se guardar segredo a respeito de todas as informações sobre as quais adquire-se conhecimento no exercício de suas profissões. No Brasil, a questão da manutenção do segredo profissional das profissões de saúde adquire um caráter dramático quando se leva em consideração a implementação da Troca de Informações em Saúde Suplementar por parte da Agência Nacional de Saúde Suplementar, autarquia especial que regula o setor de saúde suplementar. Pretendendo facilitar a troca de informações entre prestadores de serviços e operadoras, e também permitir e homogeneizar a obtenção de informação para o estabelecimento de políticas públicas, a Troca de Informações em Saúde Suplementar já é realizada desde 2008, envolvendo todas as informações de saúde de mais de 52 milhões de beneficiários. A utilização de tecnologias de troca de informação e a criação de bancos de dados, associados a um histórico de vazamento de dados sensíveis, criam dúvidas sobre a manutenção do segredo profissional e o caráter privado das informações de saúde. Neste trabalho, foi analisada a legislação estruturante da Troca de Informações em Saúde Suplementar no que diz respeito aos requisitos de segurança para a troca e armazenamento de informação sensível com o intuito de verificar se essa legislação supre, de modo eficaz, a exigência

de proteção à manutenção do caráter privativo das informações de saúde que existe nos Códigos de Ética Profissionais e no Código Civil Brasileiro. Apesar das exigências para a segurança das informações ser, hoje, adequada à manutenção do segredo profissional enquanto essas informações são trocadas ou encontram-se armazenadas nas operadoras de planos de saúde, a norma se fia nos requisitos estabelecidos por um órgão privado – cujas prioridades, naturalmente, podem, no futuro, não estar vinculadas exclusivamente ao maior bem social. Ademais, não se observa na legislação uma atenção ou recomendações dedicadas ao profissional em consultório isolado e que armazena os dados de seus pacientes em computadores pessoais previamente ao envio via internet. Além disso, em consultas realizadas à ANS em agosto e setembro de 2009 a respeito dos dados transmitidos pelas operadoras à Agência para o cumprimento do disposto nos artigos 20 e 32 da lei 9656/98, não se obteve resposta a respeito de quais dados são repassados pelas operadoras à ANS, nem sobre quais os padrões de segurança a que estes dados estão submetidos, nem, tampouco, sobre quais os indivíduos que têm acesso a estes dados, indicando falta da necessária transparência que é essencial a uma autarquia regulatória de um setor de interesse social. Estes fatos indicam claramente que a manutenção do segredo profissional está em risco nas atuais condições.

Palavras-chave: gestão de segurança em sistemas computacionais, segredo profissional, responsabilidade pela informação, Agência Nacional de Saúde Suplementar (Brasil)

ABSTRACT

Jacob CH. Analysis of the use of new technologies in the exchange and storage of health information and in relation to the professional secrecy [dissertation]. São Paulo: Universidade de São Paulo, Faculdade de Odontologia; 2009.

Health information is valued and recognized as sensible and private since ancient times. It is also considered one of the most important factors in maintaining and supporting the fabric of society, the constitutional guarantee of liberty and also, democracy itself. Health professionals have the duty to keep all their patient's information private. In Brazil, this acquires a dramatic character when one considers the recently implemented Information Exchange in Supplementary Health (TISS) by the Agência Nacional de Saúde Suplementar, government's regulating bureau for the supplementary health sector. Intending to facilitate the information exchange between service providers and health operators, and also to standardize the process of obtaining and providing information for policy makers, the Information Exchange has been in use since 2008 and involves identifiable health information of more than 52 million users. Technologies to allow health information exchange and the creation of data banks associated with sensible information data leaks raise doubts over the ability to keep health information safe from prying eyes. In this study, the structural legislation of the Information Exchange in Supplementary Health was analysed regarding the safety requirements proposed for the health information exchange and storage, to verify if it addresses the demand – that exists in professional codes of ethics and also in Brazil's Código Civil – to protect the privacy of health information. Although - by today's standards - the requirements for information security are deemed adequate for the safekeeping and in addressing the need for privacy and security while the information is exchanged or stored by the health plans operators, there's no dedicated attention to recommendations for

the professionals on their small practice offices, who hold their patients information on their personal computers. Also, the law establishes that a private agency is responsible for dictating the requirements that keep the information safe, a measure that is not entirely risk-safe as the interests of the private sector may shift with the market, leaving the social needs/interests behind. Besides these facts, when consulting the Agência Nacional de Saúde Suplementar in august and september 2009 regarding what kind of data is transmitted by the Health Plans operators and what kind of security measures are undertaken to protect this data, no answer was obtained, indicating a lack of transparency that is appalling in a regulatory bureau that serves the society. These facts clearly indicate that the maintenance of professional secrecy and patient privacy is threatened in current conditions.

Keywords: computer systems security management, professional secrecy, information accountability, Agência Nacional de Saúde Suplementar (Brazil)

LISTA DE ABREVIATURAS

ANS	Agência Nacional de Saúde
BID	Banco Interamericano de Desenvolvimento
CC	Código Civil
CEO	Código de Ética Odontológico
CF	Constituição Federal
CFM	Conselho Federal de Medicina
CFO	Conselho Federal de Odontologia
CIH	Comunicação de Internação Hospitalar
CNES	Cadastro Nacional de estabelecimentos de Saúde
CNS	Cartão Nacional de Saúde
CONASS	Conselho Nacional de Secretários de Saúde
CP	Código Penal
ETP	Electronic transfer of prescriptions
GTO	Guia de Tratamento Odontológico
HIPAA	Health insurance portability and accountability act
IAPs	Institutos de Aposentadorias e Pensões
MP	Medida provisória
MS	Ministério da Saúde
NGS	Nível de Garantia de Segurança
NHS	National Health System
RDC	Resolução da Diretoria Colegiada
RN	Resolução Normativa
SIA	Sistema de Informações Ambulatoriais
SIB	Sistema de Informações de Beneficiários
SIH	Sistema de Informações Hospitalares
SIM	Sistema de Informação de Mortalidade
SINAN	Sistema Nacional de Agravos de Notificação
SINASC	Sistema Nacional de Nascidos Vivos
SIP	Sistema de Informações de Produtos
SUS	Sistema Único de Saúde
TI	Tecnologia de informação
TISS	Troca de Informações em Saúde Suplementar

SUMÁRIO

1 INTRODUÇÃO	12
2 PROPOSIÇÃO	16
3 REVISÃO DE LITERATURA	18
3.1 Panorama Geral	19
3.2 O direito à privacidade e a importância de sua manutenção	25
3.3 Base deontológica para a manutenção do segredo profissional	29
3.4 Breve histórico do setor de saúde suplementar no Brasil	30
3.4.1 regulamentação do setor de saúde suplementar	32
3.5 Informação e Saúde Suplementar	35
3.6 Quebras recentes do caráter sigiloso das informações em bancos de dados no mundo	43
4 MATERIAL E MÉTODO	46
4.1 Material	47
4.2 Método	48
5 DISCUSSÃO	49
5.1 Requisitos de segurança e a legislação estruturante da TISS: Resoluções Normativas 114 e 153 da ANS	51
5.1.1 Resolução Normativa 21 da ANS, de 12 de dezembro de 2002	53
5.1.2 Resolução da Diretoria Colegiada 64 da ANS, de 10 de abril de 2001	53
5.1.3 Manual de Certificação para Sistemas de Registro Eletrônico em Saúde	55
5.2 Das informações enviadas pelas operadoras à ANS	61
6 CONCLUSÕES	63
REFERÊNCIAS	65
ANEXOS	71

INTRODUÇÃO

1 INTRODUÇÃO

A obtenção e processamento de informação, no mundo contemporâneo, é essencial para a manutenção da competitividade não apenas dos estados, como também dos atores econômicos, sejam pessoas físicas ou jurídicas.

Historicamente, e precedendo as formas tradicionais de Estado, toda informação obtida pelo que podemos chamar de formas soberanas de governo era usada para a manutenção de seu status frente a outras formas soberanas de governo. Na antigüidade pré-histórica, para a ampliação de suas zonas de caça, coleta e cultivo de alimento; posteriormente - e até hoje, para o aumento de sua capacidade de projeção de poder e controle territorial (Aron, 1986).

Na contemporaneidade, a informação também possui importância estratégica não apenas para os Estados Nacionais, circunstância em que a informação é coletada por agências governamentais especializadas tanto para estabelecer políticas públicas ou diretrizes de estratégia internacional; mas também para os atores econômicos que, inseridos em um panorama extremamente competitivo, não podem se dar ao luxo de agir e planejar suas ações apenas de acordo com suposições, por conta disso, valorizam a obtenção de informação sobre o mercado consumidor cada vez mais, fazendo uso de empresas especializadas em pesquisa de campo e *data-mining*.

No início do século XXI, a informação é uma *commoditie*, quantificada, avaliada e comercializada. É nesse contexto, em que a troca e a possibilidade de obtenção de informação é mais e mais comum, que a sociedade depara-se com um paradoxo: Se, por um lado, o amadurecimento das relações democráticas leva a um maior controle da sociedade sobre o Estado, a evolução tecnológica, por outro lado, dá ao Estado contemporâneo a possibilidade de controle e observação da sociedade e do indivíduo em seu contexto social (e mesmo privado) que não encontra precedentes em toda a história da humanidade.

Este controle e capacidade de observação por parte do Estado pode servir

a uma diversa gama de interesses, que podem variar (mas não são limitados) desde a avaliação e controle de riscos epidemiológicos até mesmo, no caso de Estados-policiais, o controle ideológico das manifestações políticas de determinado população. Como exemplo disso, autores como A. Huxley e G. Orwell criaram toda um conjunto de obras em que alertam para os perigos da ausência de limites e pouca regulação para a obtenção e armazenamento de informação dos cidadãos em Estados com poderes quase ilimitados nos períodos entre- e pós-guerra, no século XX.

Dentre as informações pessoais obtidas e armazenadas pelo Estado, temos hoje, em especial, as informações de saúde, cujo teor é tradicionalmente protegido de acordo com o juramento hipocrático e, deontologicamente, pelos códigos de ética profissional.

A proteção às informações pessoais de pacientes é, hoje, característica indissociável das profissões da área da saúde, dentre as quais a odontologia é um exemplo, com o segredo profissional e a guarda das informações de saúde dos pacientes protegidos pelo código de ética odontológico em seus artigos 3º, 5º e 10º.

A dicotomia entre a necessidade da obtenção de informações pessoais por parte do Estado para os mais diversos fins e a necessidade de manutenção do segredo profissional resulta em um campo em que interesses conflitantes se embatem, sem que haja, até o presente momento, um consenso sobre os limites de atuação das iniciativas pública e privada na coleta e utilização das informações privadas em relação à legislação que mantém a proteção às informações pessoais e ao segredo profissional.

É neste contexto, em que o avanço tecnológico permite ao Estado – e a outros atores da iniciativa privada – o acúmulo quase sem limites de informação a respeito dos cidadãos, que pretendemos analisar o estado atual da questão delimitada pela necessidade de manutenção do segredo profissional do cirurgião-dentista em face das demandas, por parte do governo brasileiro, através da Agência Nacional de Saúde Suplementar (ANS) e do Ministério da Saúde, do envio dos dados obtidos pelos profissionais da saúde, em especial os cirurgiões-dentistas,

relativos às informações de saúde dos beneficiários/clientes de operadoras de planos de saúde.

PROPOSIÇÃO

2 PROPOSIÇÃO

Realizar o levantamento do estado atual da questão da manutenção do segredo profissional do cirurgião-dentista e do direito à privacidade do paciente frente aos desafios impostos pelas novas tecnologias de coleta, armazenamento e troca de dados na área da saúde, particularmente com relação à adoção do sistema de Troca de Informações em Saúde Suplementar – TISS, pela Agência Nacional de Saúde.

REVISÃO DE LITERATURA

3 REVISÃO DE LITERATURA

3.1 Panorama Geral

O direito à privacidade é um dos direitos individuais mais importantes nas sociedades, tanto por seu valor intrínseco, à medida em que o convívio social sem a existência da privacidade é tido como dificultoso, quanto pela percepção de sua importância em um mundo em que as ações humanas vêm sendo cada vez mais monitoradas (Learning to live with big brother, 2007).

Ensina Béjar (1995) que o primeiro homem a fechar uma porta para isolar-se de seu entorno desvelou a esfera privada, cuja importância e proteção encontram seu lugar no Direito.

A importância do segredo profissional, explicitado pela primeira vez no juramento hipocrático, vem sendo reconhecida ao longo dos tempos. A sua guarda, tradicionalmente, é objeto dos Códigos de Ética profissionais, e a eficiência de sua proteção passa a ser motivo de preocupação diante da evolução de novas tecnologias digitais.

No Brasil, profissões da área da saúde como medicina, odontologia, fisioterapia, terapia ocupacional, psicologia, farmácia possuem, em seus Códigos de Ética profissional, diretrizes específicas para a manutenção do segredo profissional e da privacidade dos pacientes.

Nas últimas décadas tivemos um rápido desenvolvimento e barateamento dos sistemas de computação e comunicação eletrônica, o que proporcionou sua utilização - na área da saúde - para o armazenamento, transmissão e análise dos dados de pacientes. No bojo da disseminação dos sistemas de computação e bancos de dados epidemiológicos, a preocupação com a manutenção do sigilo

profissional e da privacidade dos indivíduos tem ganhado força devido à maior possibilidade de acesso a estas informações por parte de terceiros.

No caso dos bancos de dados epidemiológicos, a troca eletrônica de informações entre os prestadores de serviços de saúde e os responsáveis pela guarda destas informações - assim como os próprios mecanismos de armazenamento de dados - podem representar ameaças à manutenção da privacidade do indivíduo e ao dever profissional de manter o sigilo, pois, como ensinam Cheswick, Bellovin e Rubin (2003), não existe segurança absoluta em sistemas eletrônicos de comunicação e armazenamento de dados.

A troca de informações de saúde através de meio eletrônico no exterior já é realizada em alguns países, enquanto outros a estão implantando. No Reino Unido, o Serviço Nacional de Saúde (NHS) propôs o *Connected for Health*, um programa de implementação de sistemas de tecnologia de informação que prevê a prescrição, registro, troca de informação entre os profissionais de saúde e a obtenção do consentimento do paciente com o uso de meio digital (British Medical Association, 2007). Na Alemanha, foi anunciada em 2005 uma estratégia nacional de implantação de tecnologia de informação em saúde para prescrição eletrônica e armazenamento (voluntário) de dados de saúde em *smartcards*. Em diversos outros países da Europa, além de Austrália e Canadá, os governos nacionais estão investindo em sistemas de Tecnologia da Informação (TI) para modernização e troca de informações no sistema público de saúde (Brasil, 2007a).

No Brasil, a Agência Nacional de Saúde Suplementar (ANS) estabeleceu um padrão de Troca de Informação em Saúde Suplementar (TISS) para registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde a partir do ano de 2007, baseando-se na análise das guias trocadas entre operadoras e prestadores e nos padrões de troca de informações já em uso em outros países (Brasil, 2005a, 2006b)

Levando em consideração a heterogeneidade entre os planos de saúde existentes e também a existência de planos de saúde com atendimento

exclusivamente odontológico, a ANS segmentou a utilização da TISS para permitir que também as operadoras de planos de saúde exclusivamente odontológicos pudessem se adequar à utilização do padrão.

É no contexto da adoção mais generalizada do uso de sistemas de informação de saúde que Ball, Chadwick e Mundy (2003) observam que a mudança dos sistemas baseados em papel para os mecanismos digitais significa que as informações pessoais serão tornadas mais facilmente acessíveis e mais difíceis de serem protegidas.

A privacidade e a confidencialidade são princípios complexos que se relacionam. A privacidade consiste no conjunto de informações sobre uma pessoa, que pode decidir mantê-las sob seu controle, ou comunicar, decidindo em que medida, a quem, quando, onde e em quais condições o outro poderá acessá-las. Já a confidencialidade se relaciona à garantia de que as informações confiadas não serão reveladas sem prévia autorização da pessoa em questão (Abdalla, 2007).

De acordo com Almeida e Muñoz (1998) há diversos motivos para o princípio do segredo profissional haver se mantido incólume ao longo do tempo. Entendem os autores que uma das principais razões para os profissionais manterem secretas as informações de seus pacientes é o peso da tradição, isto é, o profissional sente-se comprometido conceitualmente com a razão hipocrática. Afirmam também que a esta motivação há outras subjacentes, como a utilitarista, que explica que o médico mantém em sigilo as confidências dos pacientes pois estes buscarão ajuda sem medo de serem estigmatizados ou sofrerem repercussões negativas que possam resultar do conhecimento público de seus problemas, o que acaba por reforçar os aspectos de confiança mútua, assim, o profissional sabe que o paciente revelará tudo sem reservas e o paciente sabe que suas informações estarão protegidas. Os autores destacam também a motivação contratual, de caráter jurídico, que afirma haver um contrato tácito entre o médico e seu paciente, em que o primeiro só adquire a informação do o paciente, no entendimento, por este, de que ela será mantida secreta.

Neste mesmo sentido, explica Souza (2005) que:

sigilo médico profissional é dever inerente ao desempenho da profissão médica, caracterizando, a sua violação, infração ética, penal e mesmo cível. Na área do Direito Civil é cabível, juridicamente, a responsabilização – reparação - caso haja dano material ou moral ao paciente que tiver os seus dados clínicos tornados públicos. [...] e, além disso, mesmo em juízo, não precisa, nem pode o médico abrir mão do segredo profissional, o sigilo médico, salvo se amparado pelo artigo 207, do Código de Processo Penal brasileiro ('São proibidas de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho.'), resolver testemunhar, pois o paciente abriu mão do segredo. Mas, mesmo que o paciente de cujos dados tenha que fazer guarda pelo sigilo o libere, o médico só prestará as informações se assim o quiser.

Nas profissões da área da saúde, de acordo com Sacardo (2001) a privacidade constitui o mecanismo de regulação do relacionamento entre os profissionais da área da saúde e seus pacientes, que pode facilitar o estabelecimento de confiança mútua necessária para o desenvolvimento do trabalho.

Sacardo e Fortes (2000) afirmam que a informação no campo da saúde é necessária tanto para o planejamento, organização e bom funcionamento dos serviços de saúde e auditoria das atividades realizadas como para o conhecimento da morbidade e mortalidade dos grupos populacionais.

Seguindo essa linha de raciocínio, a ANS afirma que a maior disponibilidade de informação otimiza as avaliações clínicas, epidemiológicas e gerenciais; dá embasamento ao planejamento e decisões de políticas públicas da ANS e de outros órgãos e instituições governamentais (Brasil, 2008b).

No Reino Unido, Ball, Chadwick e Mundy (2003) relatam que o governo britânico introduziu um plano para a reforma do Sistema Nacional de Saúde (NHS) que inclui a mudança dos sistemas de papel para um sistema nacional de transferência eletrônica de prescrições (ETP) - o que gera preocupação em relação à manutenção da privacidade dos pacientes pela possibilidade do abuso ao acesso das informações contidas nos sistemas agregadores de dados.

Robling et al. (2004) fizeram um estudo exploratório a respeito do acesso aos dados de pacientes do setor de saúde britânico e identificaram que há preocupação pública quando, sem que haja consentimento dos pacientes, registros de saúde são

acessados para fins de pesquisa e possível publicação; quando há possibilidade de transferência de dados pessoais dos pacientes para um grupo de pesquisadores externo e quando há transferência das informações de saúde dos pacientes a uma base de dados epidemiológica externa.

Choi et al. (2006) afirmam que a “era da informação eletrônica” tem criado ondas de choque em todas as áreas da vida humana, do uso de programas de compartilhamento de arquivos ao comércio eletrônico e mesmo serviços de *internet banking*, as redes de computadores são parte integral nas vidas de milhões de pessoas e que uma área que é cada vez mais afetada pela tecnologia de informação é a de cuidados de saúde. O uso de computadores para armazenar e transmitir eletronicamente os dados de pacientes tem revolucionado o sistema de saúde, mas, à medida que as informações de saúde são processadas, armazenadas e transmitidas eletronicamente, novas ameaças à proteção dos indivíduos tornam-se evidentes.

Estes autores também relatam que enquanto os benefícios pelo armazenamento e transmissão eletrônicos são incontáveis, estes ganhos não podem ser aceitos às custas da privacidade do indivíduo, e que medidas de proteção para assegurar e proteger o caráter privado das informações de saúde devem ser tomadas.

Al-Shahi e Warlow (2000) alertam que a consulta à população é necessária para determinar o equilíbrio entre a proteção aos dados individuais e o uso legítimo destas informações em pesquisas sem que haja a necessidade do consentimento de cada pessoa em todas as ocasiões.

Damschroder et al. (2007) esclarecem que o padrão norte-americano de troca eletrônica de informações em saúde foi estabelecido em 1996 pela Lei de Seguro de Saúde, Portabilidade e Confiabilidade (HIPAA), uma lei que especifica os padrões de segurança e privacidade para transações eletrônicas no que diz respeito aos dados dos pacientes para todos os prestadores de serviços de saúde. De modo geral, a HIPAA possui dispositivos que têm por objetivo a proteção das informações dos indivíduos ao estabelecer como e quando estas informações

podem ser reveladas e por quais razões. Schneier (2005) esclarece que as sanções à quebra da privacidade dos prontuários de saúde são de penalidades civis contra companhias que não se adequam às regulações e penas criminais contra indivíduos e corporações que propositadamente se apropriam ou usam de modo inadequado os dados dos pacientes.

Damschroder et al. (2007) alegam que, apesar de muitos pesquisadores acreditarem que as limitações à liberação de dados de prontuários médicos de pacientes impostas pela HIPAA terem sido excessivas, os pacientes estão dispostos a fornecer suas informações desde que mantenham o controle sobre quais informações serão liberadas, a quem, bem como a que tipo de pesquisa e em que condições.

Krishna, Kelleher e Stahlberg (2007) destacam que nos Estados Unidos, enquanto a rápida digitalização de prontuários de saúde e bases de dados administrativas prometem tornar os estudos epidemiológicos mais eficientes do que jamais foram para melhoria da prestação de serviços de saúde, o uso dos dados de pacientes levanta a preocupação a respeito da confidencialidade e riscos institucionais.

No Brasil, Dallari (2007) traça paralelos entre a necessidade do consentimento livre e esclarecido do indivíduo sujeito à pesquisa e a necessidade de os sistemas de coleta de informação das bases de dados epidemiológicos aceitarem a eventual recusa por parte da pessoa em tornar disponíveis as informações de seus dados clínicos, sem que haja quaisquer prejuízos ao seu atendimento. O autor destaca, também, a necessidade de serem estabelecidas medidas para a proteção da confidencialidade das informações, de modo a manter assegurada a garantia da preservação do sigilo.

Afirma Louzã (1995) que o desenvolvimento tecnológico tem permitido que as fichas clínicas, arquivos e prontuários sejam armazenados em bancos de dados que permitem o acesso online às informações, as quais, devido a seu caráter sensível, exigem medidas para a manutenção do sigilo. O autor também lembra

que a Constituição brasileira assegura a todos os cidadãos o *habeas data*, ou seja, o direito de conhecer as informações relativas a sua pessoa que constem em registros ou bancos de dados.

Observam Sacardo e Fortes (2000) que no Brasil

[...] a exigência de manutenção da confidencialidade e da promoção da privacidade relacionada à saúde é parte constituinte das normas deontológicas dos profissionais, em seus códigos de ética profissional.

Atualmente, entretanto, essa exigência de confidencialidade ultrapassa os limites da deontologia devido à potencial ameaça à privacidade pelos bancos de dados individuais.

Toda essa preocupação repousa na percepção da importância do foro íntimo que, de acordo com Béjar, representa para o homem a sede de sua realização enquanto indivíduo, o ponto de inflexão onde o membro da comunidade passa a enxergar em si - e nos outros - a singularidade do ser; e, para a sociedade, a fundamentação de sua legitimidade enquanto comunidade de indivíduos.

3.2 O direito à privacidade e a importância de sua manutenção

Privacidade e liberdade são princípios que se amalgamam como duas faces da mesma moeda, e é o manto de proteção dado pela privacidade que proporciona, ao indivíduo, o exercício pleno da liberdade. Privacidade e liberdade são, fundamentalmente, interdependentes. Conforme bem nos mostraram Huxley (1974) e Orwell (1972), a privacidade e a liberdade não têm lugar em um regime de excessão, que é caracterizado também pela substituição dos direitos de privacidade e liberdade por controles social, de crença, de expressão coletiva e individual.

Novais¹ (2003, apud Vieira, 2007) observa que é justamente nos Estados democráticos do pós-guerra que se desenvolve, mesmo que difusamente, a noção de que os direitos fundamentais constituem, no seu conjunto, uma ordem objetiva de valores - e dessa noção é possível extrair não apenas o dever do Estado de, além de evitar intervir na vida privada de cada indivíduo, também desenvolver mecanismos para evitar as eventuais ameaças e permitir o exercício efetivo destes direito.

É importante destacar, também, que enquanto a noção de privacidade pode ser tão antiga quanto o homem, o aspecto doutrinário do direito à privacidade pode ser traçado à Inglaterra de meados do século XVI, com o princípio de inviolabilidade de domicílio.

Observa Vieira (2007), entretanto, que foi com a publicação de um estudo analítico sobre precedentes judiciais da Suprema Corte dos EUA em fins do século 19 - a partir dos quais era possível extrair o estatuto de um direito geral à privacidade, defendendo com isso a necessidade de reconhecimento de um 'direito à privacidade', ou seja, o direito do indivíduo de estar só com seus pensamentos, emoções e sentimentos, independentemente da forma de expressão - que o avanço doutrinário ganhou força.

Após a 2ª Guerra Mundial, o direito à privacidade ganha contornos internacionais, sendo reconhecido na redação de diversas declarações e convenções: na Declaração Universal dos Direitos do Homem, de 10 de dezembro de 1948; novamente no texto da Convenção para Proteção dos Direitos do Homem e das Liberdades Fundamentais em Roma, 1950; em 1966 no Pacto Internacional de Direitos Civis e Políticos; e, em 1969 na Convenção Americana sobre Direitos Humanos (Vieira, 2007).

Com o reconhecimento no plano internacional, aos poucos o direito à privacidade foi - e continua sendo - incorporado ao ordenamento jurídico de cada país.

¹ Novais JR. As restrições aos direitos fundamentais não expressamente autorizadas pela constituição. Coimbra: Coimbra Editora; 2003. p. 63-4.

Na Constituição da República Federativa do Brasil (Brasil, 1988), apesar de não haver dispositivo a respeito da proteção da privacidade de forma específica, o Título II - Dos Direitos e Garantias Fundamentais em seu artigo 5º, inciso X estabelece como "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

No direito brasileiro, Costa Jr. (2004) faz uma diferenciação entre proteção da honra e proteção da privacidade ao afirmar que a proteção da honra refere-se à proteção do bom-nome frente aos outros membros da sociedade, enquanto a proteção da privacidade diz respeito à individualidade, à preservação, por parte do indivíduo, dos aspectos interiores que a intromissão alheia viria a perturbar. Como indivíduo, o cidadão relaciona-se com seus semelhantes. Como ser privado, o cidadão se recolhe à sua intimidade ou recato, no isolamento moral, convivendo consigo mesmo.

Já Bastos e Martins (1989) em seus "Comentários à Constituição do Brasil" procuram definir a privacidade como:

a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como impedir-lhes o acesso a informações sobre privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

Como prerrogativa da privacidade, Jabur (2000) destaca que o indivíduo pode escolher excluir, do conhecimento de terceiros, informações que deseja preservar para si, resguardando a própria imagem à publicidade não desejada.

É Vieira (2007) que, em estudo sobre o direito à privacidade na sociedade da informação, afirma:

O direito à privacidade traduz-se na faculdade que cada pessoa tem de obstar a intromissão de estranhos na sua intimidade e vida privada, assim como a prerrogativa de cada um controlar suas informações pessoais, evitando acesso e a divulgação não autorizada, configurando a intromissão por terceiros na privacidade de um indivíduo também o acesso não autorizado ou a divulgação indevida de informação. No primeiro caso, a aquisição dos dados pessoais é ilegítima; no segundo, mesmo que legítima a aquisição dessas informações, não é lícita sua ulterior revelação. Neste caso, o ato ilícito ocorre por meio da difusão não autorizada da intimidade alheia.

Também Costa Jr. (2004) discorre a respeito destas duas formas de violação da privacidade:

Na expressão “direito à intimidade” são tutelados dois interesses, que se somam: o interesse de que a intimidade não venha a sofrer agressões e de que não venha a ser divulgada. O direito, porém, é o mesmo. O que pode assumir uma gama diversa é o interesse protegido pelo direito. São duas esferas de interesses, abarcadas pelo mesmo raio de proteção do mesmo direito. No âmbito do direito à intimidade, portanto, podem ser vislumbrados esses dois aspectos: a invasão e a divulgação não autorizada da intimidade legitimamente conquistada. Em termos de conteúdo, todavia, não deve prevalecer a distinção.

Relata Vieira (2007) que um outro exemplo de quebra da privacidade ocorre quando é possível identificar o indivíduo a partir de informação legitimamente adquirida, mesmo quando o acesso a tal informação é legítimo e permitido mas à identificação não é, como por exemplo, no caso de um estudo epidemiológico em que é possível ligar a informação armazenada sem a identificação do indivíduo a um conjunto de dados que permitem identificá-lo.

Como ponto de maior importância ao exercício das profissões da área da saúde, temos que a privacidade proporciona ao indivíduo a oportunidade de desvencilhar-se das máscaras que lhe impõe a sociedade, conferindo-lhe um espaço reservado em que pode explorar e expor livremente o que o aflige, sem o temor de represálias externas que poderiam ocorrer caso essas informações se tornassem de domínio público.

Ortega y Gasset (1981) ressalta a necessidade do ser humano em introjetar-se, de concentrar-se, chamando a esse processo “ensimesmamento”, da percepção clara de que “eu” sou diferente do “outro”, e que me constituo como “eu” a partir das minhas relações com este “outro”. A privacidade impõe-se, assim, como condição *sine qua non* para o desenvolvimento do senso de individualidade.

Vieira (2007) destaca que a privacidade é necessária para possibilitar, à pessoa, a expressão de seus sentimentos sem constrangimentos na medida em que sem essa condição não dispõe de espaço íntimo para deixar de representar os papéis que exhibe no cotidiano social. Abandonados os disfarces, o indivíduo pode finalmente exercer a auto-avaliação.

A garantia de manutenção da privacidade constitui um fator de inestimável importância para permitir ao paciente revelar, ao profissional que o atende, informações que melhor seriam mantidas em sigilo para o convívio social, mas que, no contexto do atendimento de saúde podem ser essenciais para o estabelecimento de determinado procedimento terapêutico.

3.3 Base deontológica para a manutenção do segredo profissional

O caráter privativo e íntimo das informações derivadas do atendimento de saúde é previsto, ao menos, desde a antiguidade clássica, no código hipocrático. Ao longo do tempo, mesmo com diferentes adaptações e interpretações durante a idade média e no período moderno, a manutenção do segredo profissional sempre foi alvo de grande atenção, em relação a sua importância para a prática médica e para a sociedade.

No período contemporâneo, com a regulamentação das profissões da área da saúde pelo Estado, a manutenção do segredo profissional é prevista nos Códigos de Ética de diversas profissões da área da saúde. No caso da odontologia, o segredo profissional tem um caráter duplo. De acordo com o artigo 3º, Inciso II e artigo 5º, inciso VI do Código de Ética Odontológico (CEO), em sua redação de 2006 o cirurgião-dentista tem, respectivamente, o direito e dever de resguardar e guardar o segredo profissional, mantendo sob sigilo as informações prestadas pelo paciente salvo nos casos previstos nos parágrafos 1º e 2º do artigo 10º do CEO abaixo transcritos:

- § 1º. Compreende-se como justa causa, principalmente:
- a) notificação compulsória de doença;
- b) colaboração com a justiça nos casos previstos em lei;
- c) perícia odontológica nos seus exatos limites;
- d) estrita defesa de interesse legítimo dos profissionais inscritos;

e) revelação de fato sigiloso ao responsável pelo incapaz.

§ 2º. Não constitui quebra de sigilo profissional a declinação do tratamento empreendido, na cobrança judicial de honorários profissionais.

Não havendo a justa causa para a revelação das informações de pacientes, o cirurgião-dentista ainda pode se escusar de revelar as informações requeridas alegando o disposto no artigo 144 do Código Civil Brasileiro que estabelece: “Ninguém pode ser obrigado a depor de fatos, a cujo respeito, por estado ou profissão deva guardar segredo”.

Daruge e Massini (1978) ressaltam o fato de que o Código Penal, no artigo 154, estabelece que:

revelar alguém, sem justa causa, segredo de que tem ciência em razão de função, ministério, ofício ou profissão e cuja revelação possa causar dano a outrem:

Pena - detenção de três meses a um ano, ou multa.

Esclarece também o autor que “profissão”, no sentido genérico, pode abranger todas as atividades ou ocupações exercidas pelas pessoas, para ganharem os seus meios de subsistência, em especial, neste caso, a profissão liberal do cirurgião-dentista, do médico, do engenheiro, do advogado e outras em que o profissional toma conhecimento de fatos que são parte da intimidade de seus clientes que, uma vez revelada, poderá causar danos, enquadrando o profissional entre os crimes contra a inviolabilidade dos segredos.

3.4 Breve histórico do setor de saúde suplementar no Brasil

Desde a estruturação da saúde previdenciária na década de 1940, prevalecia o modelo do seguro social organizado em torno dos Institutos de Aposentadorias e Pensões (IAPs). Esses institutos, representantes de diversas categorias de trabalhadores urbanos para a organização da oferta de saúde, em sua grande

maioria compravam a prestação de serviços de consultórios médicos ou de estabelecimentos hospitalares. Na década de 1950, com a criação de diversas empresas estatais e instalação, no país, de muitas multinacionais, surgem os sistemas assistenciais próprios, isto é, que prestavam assistência médica de forma direta a seus funcionários.

A Previdência Social, com a justificativa de que o acesso aos serviços médicos aos beneficiários era cada vez mais complexa devido à expansão da cobertura e uniformização de benefícios ocorrida na década de 50, ampliou os credenciamentos de prestadores de serviços privados de saúde por meio, principalmente, do financiamento de grupos médicos, organizando sua rede, constituída de unidades próprias e credenciadas, em dois subsistemas: um voltado ao atendimento de trabalhadores rurais e outro, para trabalhadores urbanos.

Simultaneamente, as caixas de assistência e os sistemas patronais também estendiam seus credenciamentos para atender a demanda cada vez maior por atendimentos não vinculados à Previdência Social.

O crescimento dos credenciamentos gerou conflitos no âmbito da categoria médica, que entendeu a situação criada segundo duas vertentes de análise: uma, que pretendia preservar a prática liberal da Medicina; outra, que defendia a prática médica voltada para o mercado que se apresentava. Originaram-se assim, duas modalidades de empresas médicas: as cooperativas médicas, que prestavam atendimento nos consultórios dos próprios profissionais e as medicinas de grupo, responsáveis pelos atendimentos hospitalares (Brasil, 2007d).

Desde a década de 1960, trabalhadores de estatais, bancários, algumas instituições do governo federal, entre outros, já possuíam planos de saúde. Este período é, sem dúvida, um marco divisor na história da Saúde Suplementar no Brasil.

A odontologia passa a ter um papel de maior relevância no setor de saúde suplementar a partir da década de oitenta, quando, por decorrência de diversas crises financeiras – provocaram a perda de poder aquisitivo da população – e pelo

aumento do número de faculdades de odontologia, com a maior concorrência, os cirurgiões-dentistas passam a aceitar e formalizar, em suas clínicas particulares, contratos de prestação de serviço e convênios com empresas – ou mesmo a credenciarem-se como prestadores de serviço em empresas de planos de saúde odontológicos (Garcia; Cobra, 2004).

Os planos exclusivamente odontológicos contam, hoje, com cerca de 12 milhões de associados, de um total de pouco menos de 53 milhões de beneficiários de planos de saúde suplementar em junho de 2009 (Brasil, 2006b).

3.4.1 regulamentação do setor de saúde suplementar

Durante a década de 1990, observou-se que o setor de Saúde Suplementar teve um crescimento desordenado e desregulado, o que levou à aprovação da Lei n. 9.656/98 e, posteriormente, da Lei n. 9.961/2000, que criou a Agência Nacional de Saúde Suplementar. Entre os fatores que levaram a este crescimento, podemos citar o fato de ter sido esse um período em que a conjuntura internacional vivia uma onda conservadora de reformas de cunho neoliberal, nos planos econômico, social e político, com reflexos no Brasil. Isto vem acompanhado de uma redução do papel do Estado nas políticas sociais, que ocasionou a deterioração dos serviços públicos de saúde (Brasil, 2007d).

Assim, desde a década de cinquenta, com o surgimento dos primeiros planos de saúde até o início da regulamentação setorial, em 1998, assistimos a expansão de um setor de saúde suplementar praticamente sem regras de funcionamento e sem interface com o Sistema Único de Saúde (SUS).

Em 1998, uma série de atos governamentais buscou estabelecer regras para o bom funcionamento do extremamente complexo setor de saúde suplementar.

Poucos setores da economia têm as características do setor de saúde suplementar, por tratar-se de um bem credencial e meritório, que envolve ao menos três grandes pólos de tensionamento: as operadoras de planos e seguros, os prestadores e os beneficiários (denominados também associados, usuários ou consumidores). Não se trata, em absoluto, de grandes pólos homogêneos, pois as operadoras disputam entre si os prestadores hospitalares, que nem sempre têm interesses únicos com as entidades de classe e os consumidores contam com diversas instâncias de representação, que nem sempre representam a todos de forma igualitária. Para além destas características, o Estado tem função prioritária: estabelecer políticas setoriais em harmonia com a política pública de saúde nacional. Esse debate, em si, também não é simples: basta que relembremos que uma considerável parcela dos prestadores de saúde atua tanto contratado pelo sistema público quanto pelas operadoras de planos e seguros de saúde (Brasil, 2007d).

Por conta disso, não resulta surpresa afirmar que a regulação no setor de saúde é uma ação complexa, compreendendo um considerável número de atividades, instrumentos e estratégias, levando em consideração o fato de que o setor é composto por um conjunto de serviços e programas de promoção, prevenção, tratamento e reabilitação, que incluem tanto cuidados individuais quanto coletivos e que requerem a atenção em distintos serviços de saúde ambulatoriais e hospitalares (Brasil, 2007d).

A questão da intervenção do Estado em um mercado privado sempre suscita polêmica, pois, para além da intervenção em uma atividade econômica, especificamente na área de saúde muitos ainda podem entender que, por conta da regulação, se estivesse permitindo a “mercantilização da saúde”, ou mesmo que se estivesse colocando a saúde no mesmo patamar de outros bens públicos cuja exploração foi privatizada.

Em tese, se espera que o Estado atue em nome dos cidadãos, distribuindo bens e serviços de forma a garantir a oferta de acordo com as necessidades da população, e não de acordo com o interesse do indivíduo, a pressão de determinados grupos ou ainda conduzidos exclusivamente pela demanda. Quanto

mais forte for a atuação do Estado, por meio da introdução de mecanismos de regulação, melhores devem ser os resultados em termos de qualidade, equidade e acesso, conforme pode ser observado na figura 1 (Brasil, 2007d).

Para realizar a regulação no setor de saúde suplementar, a ANS foi criada em novembro de 1999, pela Medida Provisória n. 1.928, aprovada pelo Congresso Nacional e convertida na Lei n. 9961, de 28 de janeiro de 2000. Constituída como autarquia sob o regime especial, vinculada ao Ministério da Saúde, como órgão de regulação, normatização, controle e fiscalização das atividades que garantam a assistência suplementar à saúde (Brasil, 1998, 2000).

A natureza de autarquia especial conferida à ANS é caracterizada por sua autonomia nos setores administrativo, financeiro, patrimonial e de gestão de recursos humanos, e também nas suas decisões técnicas e no mandato fixo de seus dirigentes. Sua finalidade institucional consiste em defender o interesse público na assistência suplementar à saúde, regulando as operadoras setoriais, inclusive quanto às suas relações com prestadores e consumidores.

A ANS é composta por cinco diretorias.

- Diretoria de Gestão: cuida de todo o funcionamento da ANS, incluída a gestão de pessoal, financeira e patrimonial;

Figura 1 – Quadro comparativo de mudanças provocadas pela regulamentação do setor de saúde suplementar (Brasil, 2007c).

- Diretoria de Desenvolvimento Setorial: responsável pela operacionalização do ressarcimento; pelo desenvolvimento e integração dos sistemas de informação e pela interface com o Sistema Único de Saúde;
- Diretoria de Fiscalização: responsável pelo *call center*; pelas atividades de fiscalização (reativa e pró-ativa); pela interface com os órgãos de defesa do consumidor;
- Diretoria de Normas e Habilitação das Operadoras: responsável pela autorização de funcionamento, registro e monitoramento das operadoras; pela operação dos regimes especiais (Direção Fiscal e Técnica), e do processo de liquidação extra-judicial;
- Diretoria de Normas e Habilitação dos Produtos: responsável pelo registro dos produtos; pelo monitoramento da assistência prestada; pela instrução dos processos de alegação de doença ou lesão pré-existente; pelo acompanhamento dos programas de promoção e prevenção; e ainda pelo monitoramento de preços e notas técnico-atuariais e autorização dos reajustes anuais dos planos individuais e eventuais processos de revisão técnica (Brasil, 2007d).

3.5 Informação e Saúde Suplementar

A obtenção de informação precisa e sua interpretação e disponibilização foi considerada fundamental para o conhecimento e planejamento do setor de saúde suplementar, configurando-se como ferramenta estratégica para a regulação do setor (Brasil 2008a).

A compatibilização dos bancos de dados e a obtenção e repasse de informação por parte das operadoras surgem como instrumentos de gestão que ampliam a capacidade de regulação, permitindo a construção de indicadores de qualidade

para o sistema nacional de saúde. Para o cumprimento destas metas mostrou-se necessário o desenvolvimento de um sistema padronizado de informações que viabilizasse a troca de informações entre a ANS, as operadoras de planos e prestadores.

A tendência à padronização já era observada no próprio mercado, mediante iniciativas periódicas de estudos por parte de associações representativas do setor. Essas iniciativas são relevantes para a melhoria do atendimento dos beneficiários de planos privados de assistência à saúde e para a racionalização dos procedimentos administrativos e operacionais de operadoras e prestadores. A utilização, por parte das operadoras, de uma grande variedade de formulários com informações diversas, acrescida aos demorados mecanismos de troca de informações, especialmente no que tange ao faturamento, pagamento e glosas de despesas por ambos os segmentos, além dos erros de preenchimento e do custo administrativo que tais mecanismos representam, são alegações constantes para as dificuldades de melhoria da eficiência e agilidade do atendimento (Brasil, 2005a, 2006b).

A partir da observação do setor, a Agência Nacional de Saúde Suplementar reconhece que o estabelecimento de um padrão essencial de informações é necessário para o aprimoramento da qualidade da prestação da assistência, para o aperfeiçoamento da obtenção de informações sobre o setor de saúde suplementar e para a otimização dos recursos utilizados na troca de informações entre operadoras e prestadores. Além disso, considera a sistematização de informações como um dos elementos fundamentais na construção de indicadores que permitam avaliar o estado de saúde, subsidiar o planejamento, acompanhamento e avaliação dos serviços prestados, e fornecer aos segmentos envolvidos, à ANS e ao Ministério da Saúde informações sanitárias que permitam efetuar comparações e apoiar as políticas nacionais de saúde, *verbis*: “resta o entendimento de que a regulação e a conseqüente regulamentação constituem-se num processo em evolução. E regulação, sem dúvida, requer informação.” (Brasil, 2005a).

Para atender a essas necessidades, a ANS desenvolveu um projeto com dois

objetivos. O primeiro, através de Consulta Pública, para estabelecer um padrão essencial de informações a serem trocadas entre operadoras e prestadores de serviços de saúde. O segundo objetivo, desenvolvido em convênio com o Banco Interamericano de Desenvolvimento (BID), para disponibilizar para operadoras e para os prestadores de serviços de saúde contratados um aplicativo informatizado, de uso opcional, modelado com o padrão essencial obrigatório de informações.

O estudo sobre a padronização das informações da assistência complementar à saúde desenvolvido pela ANS compreendeu: 1) revisão da bibliografia nacional e internacional sobre padronização de informações em saúde; 2) pesquisa dos padrões de informação adotados no país e no exterior; 3) revisão da legislação relacionada ao padrão estudado; 4) estudo dos padrões existentes no Cartão Nacional de Saúde (CNS/MS), Cadastro Nacional de Estabelecimentos de Saúde (CNES/MS); Sistema de Informação de Mortalidade (SIM/MS), Sistema Nacional de Nascidos Vivos (SINASC/MS), Sistema Nacional de Agravos de Notificação (SINAN/MS), Comunicação de Internação Hospitalar (CIH/MS), Sistema de Informações Hospitalares (SIH/SUS) e Sistema de Informações Ambulatoriais (SIA/SUS); 5) levantamento e análise das guias e formulários utilizados pelas operadoras para a troca de informações com prestadores; 6) elaboração de matriz com os dados constantes nas guias, nos sistemas públicos e nos sistemas de informação da ANS; 7) levantamento dos códigos e tabelas utilizadas no atendimento para parametrização e intercâmbio de dados; 8) visitas a prestadores de serviços (hospitais, clínicas odontológicas e serviços de apoio, diagnóstico e terapia); 9) especificação das funcionalidades do aplicativo; 10) apresentação da proposta de padronização à Câmara de Saúde Suplementar; e 11) oficinas nas cidades do Rio de Janeiro, Fortaleza, Curitiba, São Paulo e Porto Alegre, reunindo operadoras e prestadores de serviços de saúde para apresentação, discussão e sugestões à proposta (Brasil, 2005a).

Com as conclusões obtidas a partir dos estudos e das oficinas realizadas, a ANS definiu um padrão essencial para a troca de informações entre operadoras e prestadores de serviços de saúde, instituindo, por meio da Resolução Normativa

114, de 26 de outubro de 2005, o padrão obrigatório para a troca de informações entre operadoras de planos e seguros de saúde sobre os eventos de saúde realizados em seus beneficiários, o padrão TISS. Criou ainda, pela mesma RN, um Comitê de Padronização da Informação em Saúde, de caráter consultivo, o Copiss, que conta com a participação de entidades representativas do setor – poder público, operadoras de planos e seguros de saúde, prestadores de serviços, entidades de consumidores e instituições de ensino e pesquisa, com as seguintes funções, de acordo com o artigo V da Resolução Normativa 153 ANS de 28 de maio de 2007 – cuja íntegra pode ser consultada no Anexo B (Brasil, 2007b):

I - supervisionar, coordenar, estabelecer prioridades e propor modificações e melhorias no padrão TISS;

II - estabelecer e promover metodologia de divulgação das informações do padrão TISS;

III - revisar e aprovar termos e classificações utilizados no padrão TISS;

IV - promover, fomentar e recomendar estudos relacionados à padronização das informações em saúde complementar bem como para a troca eletrônica de informações em saúde complementar, baseados nos padrões nacionais e internacionais;

V - identificar, propor e coordenar modificações necessárias aos sistemas de informação da saúde complementar, sob coordenação da ANS, para adequação aos padrões consensuados e aos sistemas de informações de saúde do MS.

VI - propor padrões e metodologias para proteger e melhorar a confidencialidade, disponibilidade e integridade da informação em saúde complementar, bem como as boas práticas para gerenciamento seguro da informação em saúde.

§ 1º O Comitê é constituído por representantes da Agência Nacional de Saúde Suplementar, do Ministério da Saúde, das operadoras de planos privados de assistência à saúde, dos prestadores de serviços de saúde, das instituições de ensino e pesquisa, de representações de usuários, e de eventuais convidados da coordenação do Comitê de Padronização das Informações em Saúde Suplementar.

(...)

§ 3º Qualquer interessado na padronização da troca de informações em saúde, sem representatividade no Comitê de Padronização, poderá encaminhar sugestões para apreciação mediante preenchimento do modelo SOP-TISS.

Com relação à manutenção da privacidade e do segredo profissional, a Resolução Normativa 114 ANS de 26 de outubro de 2005 (Brasil, 2005b), que estabeleceu o padrão obrigatório para a troca de informações entre operadoras de plano privado de assistência à saúde e prestadores de serviços de saúde sobre os eventos de saúde, realizados em beneficiários de planos privados de assistência à saúde já trazia, em seu capítulo V, “Da Segurança e da Privacidade” a indicação

de documentos com diretrizes específicas para a proteção das informações de saúde:

Art 8º As operadoras de plano privado de assistência à saúde e prestadores de serviços de saúde devem constituir proteções administrativas, técnicas, e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial a toda informação identificada individualmente, conforme normas técnicas estabelecidas na Resolução CFM nº 1639 de 10 de julho de 2002, e na RN nº 21 de 12 de dezembro de 2002, e na RDC nº 64 de 10 de abril de 2001 ambas da ANS.

Parágrafo único. Para que os objetivos de segurança e privacidade sejam alcançados, recomenda-se que sejam observados pelo menos os requisitos de segurança do Nível de Garantia de Segurança 1 (NGS-1), descritos no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES) publicado na página da Sociedade Brasileira de Informação em Saúde - SBIS e do Conselho Federal de Medicina - CFM, conforme norma NBR ISO/IEC 17799 - Código de Prática para a Gestão da Segurança da Informação.

Pela evolução do quadro em que as mudanças propostas pelo TISS foram implementadas, e também devido ao rápido desenvolvimento técnico, a Resolução Normativa 114 foi alterada diversas vezes até ser revogada pela Resolução Normativa 153, de 28 de maio de 2007 que apresenta mudanças bastante significativas no que diz respeito à requisição de informações pela ANS e aos requisitos de segurança e privacidade em relação à RN 114, nos capítulos V e VI:

CAPÍTULO V DA REQUISIÇÃO DE INFORMAÇÕES PELA ANS

Art. 6º Toda e qualquer informação relativa a eventos de saúde, requisitada pela ANS, a partir da publicação desta Resolução, deverá ser realizada e prestada conforme previsto no padrão TISS.

§ 1º Caso a informação necessária não esteja prevista no padrão, deverá ser nele incluída através da metodologia descrita no artigo 6º desta Resolução.

§ 2º Ficam mantidas e preservadas as rotinas sistemáticas e contínuas de coleta e transmissão de dados entre as operadoras de planos privados de assistência à saúde e a ANS, bem como os requerimentos de informação, de caráter excepcional.

§ 3º O envio das informações requisitadas pela ANS não exime as operadoras nem os prestadores da obrigação de apresentar documentação comprobatória da veracidade das informações prestadas, bem como de quaisquer outros documentos e informações que a ANS, nos limites de sua competência, vier a requisitar.

CAPÍTULO VI DA SEGURANÇA E DA PRIVACIDADE

Art. 7º As operadoras de planos privados de assistência à saúde e os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial a toda informação identificada individualmente, conforme normas técnicas estabelecidas na Resolução CFM nº 1639 de 10 de julho de 2002, e na

RN nº 21 de 12 de dezembro de 2002, e na RDC nº 64 de 10 de abril de 2001 ambas da ANS.

§ 1º As operadoras de planos privados de assistência à saúde e os prestadores de serviços de saúde que optem pela forma de comunicação através da rede Internet, inclusive as que optem pela utilização de empresas intermediadoras prestadoras de serviços de conectividade, devem obrigatoriamente adotar os requisitos de segurança do Nível de Garantia de Segurança 1 (NGS-1), descritos no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES), publicado na página da Sociedade Brasileira de Informação em Saúde - SBIS, e do Conselho Federal de Medicina - CFM, conforme norma NBR ISO/IEC 17799 - Código de Prática para a Gestão da Segurança da Informação.

§ 2º Para as operadoras de planos privados de assistência à saúde e prestadores de serviços médico-hospitalares que utilizarem Webservices, recomenda-se a utilização do Nível de Garantia de Segurança 2 (NGS-2).

Art. 8º Para as transmissões remotas de dados identificados, os sistemas deverão possuir um certificado digital de aplicação única emitido por uma Autoridade Certificadora (AC) credenciada pelo Instituto Nacional de Tecnologia da Informação - ITI, responsável pela AC Raiz da estrutura da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, a fim de garantir a identidade do sistema.

§ 1º O certificado digital deve ter como um de seus atributos o Cadastro de Pessoa Física - CPF ou o Cadastro Nacional da Pessoa Jurídica - CNPJ do prestador.

§ 2º No caso de pessoa jurídica em que trabalhem vários prestadores pessoa física, todos os dados poderão trafegar sob o certificado da pessoa jurídica, devendo as operadoras manter registro do vínculo entre esses prestadores.

Com relação aos prazos para a implantação do padrão TISS, a ANS estabeleceu prazos diferenciados, iniciando pela implantação das guias padrão em papel e, a seguir, a implantação do padrão de troca eletrônica, com prazos diferentes de acordo com a complexidade do prestador de serviço.

Segundo a RN 153, o primeiro grupo a adaptar-se ao TISS consistiria em hospitais gerais e especializados, hospitais-dia e prontos-socorros gerais e especializados, clínicas e ambulatórios de especialidades, unidades de apoio ao diagnóstico e terapia, unidades móveis pré-hospitalares, unidades móveis fluviais e terrestres e policlínicas. O segundo grupo seria constituído por consultórios médicos isolados e profissionais de saúde ou pessoas jurídicas que prestam serviços em consultórios. O terceiro grupo seria constituído por clínicas radiológicas odontológicas, consultórios odontológicos isolados e cirurgiões-dentistas ou pessoas jurídicas que prestam serviços em consultórios.

A ANS afirma que a padronização e a troca eletrônica de informações em saúde suplementar trazem inúmeros benefícios, entre os quais o aprimoramento da comunicação entre os atores do setor; a redução de uso de papel, agilizando

o acesso dos beneficiários aos serviços de saúde, a facilitação da obtenção de informações para estudos epidemiológicos e definição de políticas de saúde; o favorecimento da realização de análise de custos e benefícios de investimentos na área de saúde; redução dos custos administrativos; melhoria da qualidade da assistência à saúde; possibilidade de comparação e análise de desempenho institucional resultando na otimização de recursos e aumento da qualidade de gestão (Brasil, 2006b).

Complementando a TISS, a ANS disponibilizou um software gratuito para a troca eletrônica, agregando facilidades para verificação da produção médica, controle de pagamentos, glosas e contratos, valoração de guias, além da emissão de relatórios utilizados para a entrada de parâmetros do Sistema de Informações de Produtos (SIP) e do Sistema de Informações de Beneficiários (SIB), ambos da ANS, contribuindo, assim, com o atendimento dessas normas por parte das operadoras.

A utilização desse software é opcional e seu objetivo é atender operadoras e prestadores de serviços que não possuem sistemas próprios para se adequarem ao padrão de comunicação da Troca de Informações em Saúde Suplementar - TISS.

A troca de informações em saúde suplementar de acordo com os padrões delimitados pela ANS é realizada, obrigatoriamente, pelas operadoras planos odontológicos desde maio de 2008, de acordo com os prazos estabelecidos pela RN 153. Para a odontologia, a padronização, inicialmente, foi realizada a partir de 31 de maio de 2008 com a utilização de uma guias em papel, e, a partir de 30 novembro de 2008, com a utilização do padrão de segurança em meio digital.

De acordo com o Caderno de Informações em Saúde Suplementar publicado pela Agência Nacional de Saúde Suplementar, havia, em junho de 2009, pouco menos de 12 milhões de beneficiários de planos de saúde exclusivamente odontológicos de um total de 52,7 milhões de beneficiários de planos de saúde.

Todos os tratamentos efetuados nos beneficiários de planos odontológicos devem ser registrados nas Guias de Tratamento Odontológico (Figura 2), que são

idênticas para todas as operadoras com relação à quantidade e requisitos de informação. Nesta guia é possível verificar existirem campos para a identificação do usuário do serviço de saúde, identificação da empresa do beneficiário (campo 10), identificação do beneficiário (campo 13), seu número de telefone (campo 14) e campos que ligam, diretamente, o beneficiário identificado a um plano de tratamento, inclusive com a descrição dos tratamentos a serem realizados, nos campos 30, 31 e 32 (Brasil, 2008b).

A uniformização da obtenção e processamento dessas informações através da utilização da TISS, como efeito não explicitamente citado pela Agência Nacional de Saúde Suplementar, vem a tornar também mais fácil o cumprimento do artigo 20 da lei 9656 de 3 de junho de 1998, que dispõe sobre os planos e seguros privados de assistência à saúde, e obriga as operadoras de planos de saúde

(...) a fornecer à ANS, todas as informações e estatísticas relativas às suas atividades, incluídas as de natureza cadastral, especialmente aquelas que permitam a identificação dos consumidores e de seus dependentes, incluindo seus nomes, inscrições no Cadastro de Pessoas Físicas dos titulares e Municípios em que residem, para fins do disposto no art. 32

O artigo 32 da lei 9656/98, por sua vez, diz respeito à exigência de

Logo da Empresa		GUIA TRATAMENTO ODONTOLÓGICO					Z. N° 123456789012	
1 - Preenchimento	2 - Data de Emissão do Guia	3 - Data da Autorização	4 - Nome	5 - Data Validade da Servidão	6 - Assunto ou Caso Particular			
Dados do Beneficiário								
7 - Número da Carteira	8 - Plano	9 - Empresa	10 - Data Validade da Carteira	11 - Número da Carteira Nacional de Saúde				
12 - Nome	13 - Telefone	14 - Nome do titular do plano						
Dados do Contratado Responsável pelo Tratamento								
15 - Nome do Profissional Solicitante	16 - Número do CBO	17 - UF	18 - Código CBO S					
19 - Código na Operadora (CNPJ / CPF)	20 - Nome do Contratado Encarregado	21 - Número do CBO	22 - UF	23 - Código CBO S				
24 - Nome do Profissional Remetente	25 - Número do CBO	26 - UF	27 - Código CBO S					
Plano de Tratamento / Procedimentos Solicitados / Procedimentos Executados								
28 - Tabela	29 - Código do Procedimento	30 - Descrição	31 - Quantidade US	32 - Valor US	33 - Preço/Co-participação R\$	34 - Aut. 35 - Data de Realização	36 - Assinatura	
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
37 - Data Término do Tratamento 38 - Tipo de Atendimento 39 - Tipo de Tratamento 40 - Total Quantidade US 41 - Valor Total R\$ 42 - Total Preços/Co-participação R\$								
Declara, que após ter sido devidamente esclarecido sobre as condições, riscos, custos e alternativas de tratamento, conforme acima apresentadas, aceita e autoriza a execução do tratamento, comprometendo-se a cumprir as orientações do profissional assistente e arcar com os custos previstos em contrato. Declara, ainda, que o(s) procedimento(s) descrito(s) acima, e por mim autorizado(s), foram realizados com meu consentimento e de forma satisfatória. Autoriza a Operadora a pagar em meu nome e por minha conta, ao profissional contratado que assina este documento, os valores referentes ao tratamento realizado, comprometendo-me a arcar com os custos conforme previsto em contrato.								
43 - Observação								

Figura 2 – Guia TISS do mesmo modelo utilizado atualmente pelas operadoras de planos odontológicos para a troca de informações entre o cirurgião-dentista, a operadora e a Agência Nacional de Saúde (Brasil, 2008).

ressarcimento, por parte das operadoras privadas às instituições integrantes do SUS - em relação aos serviços de atendimento à saúde prestados a seus consumidores e respectivos dependentes; e, no §2º, estabelece que para a efetivação desse ressarcimento a Agência Nacional de Saúde disponibilizará às operadoras a discriminação dos procedimentos realizados por cada instituição integrante do SUS para cada consumidor (Brasil, 1998).

3.6 Quebras do caráter sigiloso das informações em bancos de dados no mundo

Hodiernamente, temos visto diversos casos – relatados na imprensa internacional – em que informações armazenadas em meio digital tiveram o caráter de privacidade comprometido.

Condon (2008), relata que, no Reino Unido, os dados de 25 milhões de pessoas foram perdidos em outubro de 2007 pelo Her Majesty Revenue & Customs (HMR&C) apesar de todas as medidas de segurança para a proteção dos dados, como resultado de deficiências institucionais.

Na Alemanha, os dados bancários de 21 milhões de contas foram colocados à venda no mercado negro após haverem sido obtidos de modo ilícito por *hackers*, segundo Kroker, Berke e Klessea (2008).

Nos Estados Unidos, mesmo com as diretrizes de segurança para troca de informações estabelecidas pela HIPAA em 1996 há vários relatos a respeito da quebra de privacidade, como a venda dos dados de saúde de celebridades que haviam sido atendidas no Centro Médico da Universidade da Califórnia em Los Angeles (UCLA Medical Center to face sanctions after patient data breaches,

2008) e falha na manutenção da segurança dos dados de saúde da população, culminando com o evento de abril de 2009 quando a base de dados de informações de saúde do estado da Virginia foi comprometido pela ação de *hackers*, que invadiram o sistema de armazenamento, criptografaram a base de dados de 12 milhões de registros e exigiram 10 milhões de dólares como resgate para fornecer a chave de acesso e evitar a divulgação das informações pessoais.²

Blevins (2008) relata que mesmo com as regras de privacidade estabelecidas pela HIPAA a partir de 1996, os dados médicos de milhões de norte-americanos fluem livremente pela internet. A respeito disso, a União Americana de Liberdades Civis (ACLU), tradicional e respeitada entidade de defesa das liberdades constitucionais norte-americana, através de seu conselheiro legislativo senior Timothy Sparapani afirma³:

Muitos lobistas que se posicionam contra novas regras de proteção da privacidade afirmam que a lei atual de HIPAA de 1996 é suficiente e efetiva para proteger a privacidade dos pacientes. Todavia, a HIPAA diz respeito aos prontuários de saúde mas não é um estatuto de privacidade. Ela cobre apenas entidades como hospitais e companhias de seguros. Na verdade, a HIPAA tem tantos buracos que faz com que queijo suíço pareça sólido.

Johnson(2009)relata quedados pessoais de saúde provenientes de prestadores de serviço tem sido inadvertidamente liberados em redes de comunicação *peer-to-peer* com o risco potencial de poderem ser utilizados por criminosos buscando realizar roubo de identidade ou fraudes médicas e financeiras.

No Brasil, a despeito de não haver relatos a respeito do vazamento de informações de saúde, é de amplo conhecimento o caso em que uma empresa paulistana foi fechada após relatos de que vendia os endereços, telefones, contatos de pessoas próximas como vizinhos, renda presumida e, caso possuía veículos, também o número das placas, o número RENAVAN além de dados bancários e fiscais (Polícia de São Paulo fecha site que vendia dados sigilosos, 2009). Todavia, estes dados ainda podiam ser adquiridos em setembro de 2009 de acordo com uma série de reportagens jornalísticas (Site reúne dados sigilosos de cidadãos;

² cf. <http://file.sunshinepress.org:54445/virginia-ransom-2009.html> [14. set 2009].

³ cf. em <http://www.news-medical.net/news/2008/07/23/40219.aspx> [14. set 2009]

senhas são vendidas, 2009). Deve-se frisar que os dados bancários e fiscais são privativos e sigilosos, permanecendo em bancos de dados sob a tutela do Estado, sendo permitida a quebra do sigilo apenas em casos muito específicos.

MATERIAL E MÉTODO

4. MATERIAL E MÉTODO

4.1 Material

O material a ser utilizado neste trabalho é o da legislação que regula o setor da saúde suplementar no Brasil, a regulação técnica que regula a TISS, a legislação que garante a preservação da privacidade do indivíduo, a Cartilha de Segurança para Internet publicada pela CERT, a literatura publicada a respeito da importância da manutenção da privacidade e do segredo profissional assim como a que se refere aos riscos existentes na troca e armazenamento de dados em sistemas eletrônicos.

4.2 Método

O método utilizado para interpretação da legislação e documentação é o processo hermenêutico, com a reconstrução dos discursos utilizados.

O termo hermenêutica deriva da palavra grega *ερμηνευω* que pode ser compreendida como “traduzir” ou “interpretar”. A hermenêutica é geralmente utilizada para descrever um método usado para lidar com as relações entre a linguagem e a lógica de um modo formal.

Historicamente, após o fim do período Clássico e ao longo da Idade Média, a hermenêutica foi instrumentalizada no processo interpretativo de textos bíblicos,

para, a partir do sentido literal do texto, extrair comentários e redescobrir um novo sentido, desta vez alegórico, que dava a cada elemento literal um significado simbólico (Stanford encyclopedia of philosophy, 2005).

É a partir dos trabalhos de Schleiermacher e de Dilthey no século XIX que o uso do método hermenêutico para a interpretação textual geral passa a ganhar força.

O objetivo do método hermenêutico, é, assim, a compreensão de determinado objeto de estudo em profundidade. Para isso, o principal método é o círculo hermenêutico, que prevê a análise de um assunto a partir de diversas perspectivas para então interpretá-lo.

Dilthey (1996) afirma que o método pode ser explicado seqüencialmente da seguinte forma:

1) A compreensão de determinado evento, 2) a estruturação histórica e contextual deste evento e 3) a reconstrução. [...] Assim, o todo deve ser compreendido com base no particular e o particular com base no todo. Esta contradição gera o procedimento do hermeneuta. Quando aplicamos isso a um trabalho, torna-se claro que nunca compreendê-mo-lo na primeira leitura, que nos dá apenas a idéia geral. Devemos então, por isso, buscar compreender suas particularidades.

Considerando que hermenêutica pode ser definida como interpretação, a hermenêutica jurídica é a interpretação que dá sentido à norma (Tonelli, 2002). Assim, a hermenêutica jurídica, de acordo com Musetti (1999) permite ao leitor interpretar o ordenamento jurídico, revelando valores subjacentes à letra da lei.

Uma das premissas deste trabalho é a de realizar a interpretação da lei para justapor duas teses distintas, avaliá-las e, dessa avaliação, obter uma conclusão. A primeira tese consiste na idéia de que a troca de informações em saúde suplementar não oferece risco à manutenção do segredo profissional e da privacidade do paciente; a segunda, de que a troca de informações em saúde suplementar oferece, sim, riscos à manutenção daqueles dever e direito.

Esta abordagem, por sua vez, é dialética.

Este trabalho apropria-se, portanto, de duas metodologias complementares: a hermenêutica, para a análise, e a dialética, para o confronto de idéias.

Esta é a metodologia que será adotada neste trabalho.

DISCUSSÃO

5 DISCUSSÃO

Apesar de uma abordagem filosófica estrita da *privacidade* não existir ainda, como tal, a percepção, já generalizada entre os grandes pensadores, juristas e estadistas da interdependência entre privacidade e liberdade – principalmente no sentido de que uma não pode existir sem a outra – é o suficiente para tornar o valor da privacidade como essencial à realidade da existência humana.

Essa característica de interdependência desses dois valores não podia passar despercebida – e de fato não passou – na Grécia clássica, quando os valores humanistas floresciam em meio a um panorama cultural, político e filosófico extremamente favorável.

Eco (1986) afirma que é possível inferir quais são os hábitos de determinada sociedade através das leis que essa sociedade impõe a si mesma para continuar existindo. No caso da arte médica dos gregos do período clássico, encontramos uma série de recomendações no *corpus hippocraticus*, que se supõe haver sido redigido em no século 5ºa.C. Uma dessas recomendações, dentre várias, como instruções sobre a arte da cura, a proibição do aborto, a proibição da eutanásia, a proibição de tirar vantagem do moribundo, diz respeito à não revelação das informações a que o médico tem acesso durante o tratamento de determinado doente para terceiros.

Ora, ao considerarmos que a estrutura da sociedade grega é do tamanho da cidade-estado, não custa muito imaginar o que a revelação das informações – muitas vezes íntimas e pessoais – poderiam causar exatamente aquilo que Platão abomina em sua *República*: a desordem social. Assim, não é incorreto afirmar que o preceito hipocrático de manutenção do segredo sobre as informações adquiridas tem um valor essencialmente prático para a prevenção de um problema que possivelmente vinha pondo em risco a estrutura social das cidades-estados da Grécia clássica.

É certo, como afirmam Robling et al. (2004), que a consciência, por parte dos pacientes, de que as informações prestadas vão permanecer em segredo, favorece sobremaneira a revelação de informações que, apesar de poderem provocar algum tipo de constrangimento em caso de revelação à sociedade, podem ajudar o processo de diagnóstico e a tomada de medidas terapêuticas adequadas.

No que diz respeito à odontologia, é necessário dizer que sua importância para a preservação da privacidade dos pacientes não é nem marginal nem preponderante sobre as outras profissões da área de saúde cujas atividades, quando ligadas a operadoras de planos de saúde, exigem a utilização da TISS. Com pouco mais de 11 milhões de beneficiários de planos odontológicos, segundo apurado pela Agência Nacional de Saúde Suplementar em setembro de 2009, a odontologia tem uma importância complementar à de outras profissões de saúde na proteção dos dados de saúde dos pacientes, uma vez que a ficha de anamnese e o prontuário odontológico contém informações que dizem respeito não apenas aos dados pessoais e ao tratamento planejado e efetuado, mas também ao histórico de saúde do paciente, com antecedentes pessoais e familiares (Brasil, 2006a,b).

5.1 Requisitos de segurança e a legislação estruturante da TISS: Resoluções Normativas 114 e 153 da ANS

Para verificarmos, com maior propriedade, a eficácia dos requisitos de segurança de dados da TISS, devemos realizar uma análise ponto a ponto destes requisitos conforme se encontram nos artigos 7º e 8º da Resolução Normativa 153 da ANS, de 28 de maio de 2007.

Foi, entretanto, a Resolução Normativa nº 114 da ANS, de 26 de outubro de 2005, que estabeleceu o padrão TISS, indicando em seu artigo 8º, outros documentos para a manutenção da privacidade dos pacientes e do segredo

profissional, ou seja, as normas estabelecidas na Resolução Normativa nº 21 de 12 de dezembro de 2002, na RDC nº 64 de 10 de abril de 2001 (ambas da ANS), na Resolução CFM nº 1639 de 10 de julho de 2002, além da *recomendação* de observação pelo menos dos requisitos de segurança do Nível de Garantia de Segurança 1 (NGS-1), descritos no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES) publicado na página da Sociedade Brasileira de Informação em Saúde - SBIS e do Conselho Federal de Medicina - CFM.

Como evolução do texto anterior, substituindo-o, a Resolução Normativa 153 da ANS, de 28 de maio de 2007 trouxe uma nova redação para diversos capítulos que já existiam na RN 114, dentre eles o Capítulo VI (anteriormente Capítulo V), “da segurança e da privacidade”. Dentre as melhorias implementadas, a mais importante certamente é o caráter obrigatório da adoção dos requisitos de segurança do Nível de Garantia de Segurança 1 (NGS-1) descritos no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (S-RES) publicado nos *websites* da Sociedade Brasileira de Informação em Saúde (SBIS) e do Conselho Federal de Medicina (CFM). A Resolução 153 recomenda também que Operadoras que utilizem *webservices* obedeçam aos requisitos de segurança do Nível de Garantia de Segurança 2 (NGS-2).

No artigo 8º desta resolução a ANS estabelece que para as transmissões de dados identificados os sistemas deverão possuir um certificado digital emitido por uma Autoridade Certificadora (AC) credenciada pelo Instituto Nacional de Tecnologia de Informação a fim de garantir a identidade do sistema. Todavia, o que a legislação não menciona é que uma assinatura digital não pode garantir em absoluto a identidade de um sistema, mas, tão somente, que a chave do agente de origem foi utilizada. Ellison e Schneier (2000) afirmam a respeito disso que, quando escrevem a respeito da não-repudição, teóricos da criptografia sempre se esquecem de um detalhe que existe entre o usuário e sua chave: o computador. Se um computador for infectado de modo apropriado, um código malicioso pode se utilizar da chave do usuário para assinar documentos sem o conhecimento ou a

permissão do usuário. Mesmo que fosse necessário algum tipo de confirmação, o código malicioso poderia aguardar até o usuário realizar uma confirmação legítima e assinar as duas mensagens ao mesmo tempo. Os autores afirmam que ignorar tais detalhes em artigos acadêmicos pode ser legítimo, entretanto, é uma falha acreditar que computadores reais implementem, no mundo real, um ideal que é apenas teórico; é um erro acreditar que os usuários, no mundo real, se comportem exatamente como o previsto em regras.

5.1.1 Resolução Normativa 21 da ANS, de 12 de dezembro de 2002

A Resolução Normativa 153 faz menção também à Resolução Normativa 21 da ANS, de 12 de dezembro de 2002, que dispõe sobre a proteção das informações relativas à condição de saúde dos consumidores de planos privados de assistência à saúde, estabelecendo também que as operadoras de planos privados de assistência à saúde deverão manter protegidas as informações assistenciais fornecidas pelos seus consumidores ou por sua rede de prestadores, *quando acompanhadas de dados que possibilitem a sua individualização*, não podendo as mesmas ser divulgadas ou fornecidas a terceiros, salvo em casos expressamente previstos na legislação (Brasil, 2002a).

5.1.2 Resolução da Diretoria Colegiada 64 da ANS, de 10 de abril de 2001

Curiosamente, a Resolução RDC 64 de 10 de abril de 2001 dispõe apenas

sobre a proteção do sigilo médico e a designação de médico responsável pelo fluxo de informações relativas à assistência de saúde prestada aos consumidores de planos privados de assistência, não se referindo, em momento algum, às operadoras de planos exclusivamente odontológicos ou a um possível cirurgião-dentista responsável pelo fluxo de informações relativas à assistência odontológica prestada aos consumidores de planos privados de assistência odontológica. Além disso, a Resolução não deixa claro se as operadoras de planos exclusivamente odontológicos devem estabelecer um *médico* responsável pelo fluxo de informações de saúde obtidas. Conforme é possível observar (Brasil, 2001):

Considerando a importância da proteção do sigilo médico por profissional habilitado e registrado nos Conselhos Regionais de Medicina, adotou a seguinte Resolução e eu, Diretor Presidente determino a sua publicação:

Art. 1º O fluxo de informações médicas relativas à assistência prestada aos consumidores de planos privados de assistência à saúde deverá ficar sob a responsabilidade de profissional médico, especialmente designado para este fim pelas operadoras definidas no inciso II do art. 1º da Lei n.º 9.656, de 1998, de acordo com o disposto nesta resolução, com a finalidade de preservar o sigilo nos casos previstos na legislação em vigor.

Parágrafo único. Para efeito desta Resolução, o profissional de que trata o caput deste artigo será considerado como Coordenador Médico de Informações em Saúde.

Art. 2º Resguardando as prerrogativas e obrigações profissionais do Coordenador Médico de Informações em Saúde com relação ao sigilo médico, as operadoras permanecem responsáveis pelo envio das informações relativas aos beneficiários de planos de assistência à saúde respondendo pela omissão ou incorreção dos dados.

Art. 3º A indicação do Coordenador Médico de Informações em Saúde deverá ser comunicada à ANS por carta protocolizada no prazo de cinco dias úteis, a contar da data de designação.

§ 1º Sempre que ocorrer substituição do profissional designado como Coordenador Médico de Informações em Saúde, deverá ser feita, em igual prazo, nova comunicação à ANS.

§ 2º A comunicação a que se refere o caput deste artigo deverá conter as seguintes informações sobre o Coordenador Médico de Informações em Saúde:

I Nome completo;

II Natureza do vínculo do Coordenador Médico de Informações em Saúde com a operadora;

III N.º de registro no Conselho Regional de Medicina; e

IV Endereço completo, telefone e endereço eletrônico (e-mail).

É certo, entretanto, que a Resolução RDC 64 não altera as exigências de guarda do sigilo das informações de saúde obtidas pelas operadoras de planos exclusivamente odontológicos, que encontram-se obrigadas a resguardar o segredo profissional tanto pela RN 21 de 12 de dezembro de 2002 (Brasil, 2002b) quanto

pelo Código de Ética Odontológico, que, em seu Capítulo X, “Das Entidades com Atividades no Âmbito da Odontologia”, artigo 21, implica que as mesmas normas referentes à guarda do segredo profissional estabelecidas pelo CEO para os cirurgiões-dentistas nos artigos 3º, inciso II; 5º, inciso VI e 10º são também aplicáveis às operadoras de planos odontológicos:

Art. 21. Aplicam-se as disposições deste Código de Ética e as normas dos Conselhos de Odontologia a todos aqueles que exerçam a Odontologia, ainda que de forma indireta, sejam pessoas físicas ou jurídicas, clínicas, policlínicas, cooperativas, planos de assistência à saúde, convênios de qualquer forma, credenciamento, administradoras, intermediadoras, seguradoras de saúde, ou quaisquer outras entidades.

5.1.3 Manual de Certificação para Sistemas de Registro Eletrônico em Saúde

A Sociedade Brasileira de Informação em Saúde (SBIS) também mencionada na RN 114, foi fundada na década de oitenta para incentivar e promover o uso de recursos de informática e tecnologia de informação na assistência à saúde.

O Conselho Federal de Medicina, após haver sido consultado diversas vezes a respeito da validade e da possibilidade de substituição dos prontuários em papel por prontuários digitais ou digitalizados, através de sua Câmara Técnica de Informática em Saúde e Telemedicina estabeleceu convênio com a Sociedade Brasileira de Informação em Saúde para que essas entidades passassem a fornecer, conjuntamente, certificação de Sistemas de Registros Eletrônicos de Saúde (S-RES), que são definidos como “qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde.” Os detalhes do processo de certificação dos S-RES podem ser consultados no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde.

É interessante destacar que um processo de certificação, de modo geral, exige o cumprimento de determinados requisitos. A certificação realizada pelo

SBIS/CFM pode ocorrer em duas modalidades, Nível de Garantia de Segurança 1 (NGS-1) ou Nível de Garantia de Segurança 2 (NGS-2). Para o cumprimento dos requisitos de segurança da TISS, a ANS determinou, na RN 153, a obrigatoriedade de cumprimento dos requisitos de segurança do Nível de Segurança 1 (NGS-1) que, segundo a versão 2009 do Manual de Certificação para Registro Eletrônico em Saúde consistem em: 1) controle de versão do software, 2) identificação e autenticação do usuário, 3) controle de sessão do usuário, 4) autorização e controle de acesso, 5) disponibilidade do RES, 6) comunicação remota, 7) segurança dos dados, 8) auditoria, 9) documentação, 10) tempo, 11) notificação de ocorrências.

Cada um desses requisitos implica em uma série de medidas que devem ser tomadas, por parte do desenvolvedor do sistema, para o estabelecimento de padrões mínimos de segurança no armazenamento e troca de informações através de meio digital.

O controle de versão de software tem por objetivo possibilitar a verificação da versão do software utilizado, a rastreabilidade do código fonte original e permitir o retorno a uma versão anterior em caso de falhas de atualização. Isso permite o aumento de segurança e confiabilidade do sistema, a possibilidade de prevenção de falhas e facilita o processo de auditoria.

Os requisitos de “identificação e autenticação do usuário” e o “controle de sessão do usuário” são complementares e têm por objetivo evitar que um usuário não autorizado possa se conectar ao sistema e permite que cada usuário cadastrado tenha um nível de acesso às informações de acordo com sua responsabilidade. Esse processo também deve criar um arquivo de *log* que registre quem acessou o sistema ou quais alterações foram realizadas por cada usuário. É curiosa, entretanto, a recomendação para o tipo de algoritmo de *hash* utilizado seja SHA-1 ou SHA-2, uma vez que a perda de credibilidade dos algoritmos de *hash* SHA-1⁴ foi amplamente divulgada, já a partir de 2005 – e com artigos publicados em 2008 e 2009. Seu uso, em meados de 2009, deveria ser tudo, exceto recomendado. Este tópico também estabelece o requerimento de que a sessão do usuário deva ser

⁴ cf. *Cryptanalysis of SHA-1* [http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html] - setembro de 2009.

fechada após um determinado período de inatividade.

O requisito de “autorização e controle de acesso” tem como objetivo impedir o acesso ao sistema por usuários ou entidades não autenticadas e não autorizadas e garantir que o acesso ao RES só possa ser efetuado através do mecanismo de acesso adequado.

O requisito de “cópia de segurança” tem a intenção de garantir a integridade dos dados que estão arquivados em *backup*.

O requisito de “comunicação remota” tem como objetivo assegurar que os dados trocados entre computadores cliente-servidor permaneçam protegidos, sem que haja possibilidade de interceptação por terceiros, com base em controle de acesso entre componentes no processo de comunicação. Essa segurança se dá através da utilização de *Secure Sockets Layer (SSL)*, atualmente chamadas de *Transport Layer Security (TSL)*. O uso desta tecnologia representa o que há de melhor aceito para a manutenção da segurança das informações enquanto são trocadas através da internet (Ball; Chadwick; Mundy, 2003; Ellison; Schneier, 2000).

O requisito de “segurança dos dados” declara ser necessário, quando um RES é importado de outro sistema, a identificação do profissional que realizou a importação e, no RES importado, a identificação do paciente e do médico que o atendeu. Este requisito também estabelece que todos os RES devem permanecer criptografados e que devem existir restrições à exportação de RES, permitindo que tal ação ocorra apenas quando necessário. Outras características desse requisito consistem na exigência de que os dados dos RES não possam ser alterados ou excluídos, permitindo apenas que as correções sejam feitas sem apagar os registros anteriores, evitando que usuários ou falhas no sistema possam gerar inconsistências.

O requisito de “Auditoria” estabelece que devem ser estabelecidos mecanismos que permitam: a auditoria de acesso e modificação de dados em parte ou no todo do RES; manter a integridade das trilhas de auditoria, sem a possibilidade de

alteração das mesmas, e cujo acesso deve ser permitido apenas ao auditor.

Além dos requisitos elencados, o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde também estabelece a necessidade de criação de documentação que consista em manuais de instalação, de usuário, do administrador, de mecanismos de segurança e de práticas de segurança; de representação de formato de tempo de acordo com a ISO 8601 além da necessidade de criação de interface para que usuários notifiquem a ocorrência de incidentes de segurança, problemas ou sugestões para melhoria do sistema.

Por haverem sido baseados prioritariamente nas normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002, que são, atualmente, os padrões mais utilizados no mundo para os sistemas e para a prática de gestão da segurança da informação, os requisitos impostos pelo NGS-1 do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde são consistentes com sua proposta de proteger a informação *enquanto é trocada e durante seu armazenamento* nos bancos de dados de uma operadora.

A simples existência desses requisitos, todavia, não garante a manutenção da segurança dos dados (e, por consequência, do segredo profissional e da privacidade dos pacientes) já que não há especificações, de espécie alguma, sobre como se dará a fiscalização sobre as medidas efetivamente tomadas por cada operadora.

Da mesma forma, a Resolução Normativa 153 deixa de estabelecer requisitos específicos e recomendações para a manutenção de segurança dos dados no ponto de origem da transmissão desses dados, seja ele um consultório odontológico ou uma policlínica – mantendo, ao invés disso, as mesmas recomendações para o prestador de serviço e as operadoras.

Não há como negar que a gestão de negócios, capacidade financeira e o número de RES armazenados em uma operadora são muito diferentes de seus similares em consultórios isolados, por exemplo. Da mesma forma, os requisitos de segurança, apesar de possuírem similitude, devem levar em consideração

as diferenças de complexidade entre os prestadores e as operadoras. Não há sentido em exigir de um prestador, como um cirurgião-dentista em seu consultório, que siga o disposto no NGS-1, quando seria muito mais importante – para não dizer menos custoso e mais simples – manter o computador utilizado na troca de informações livre de *software* maliciosos, que pode por em risco o caráter privado das informações armazenadas, através do uso de firewalls e programas antivírus.

Costuma-se afirmar, com muita razão, que uma corrente é tão forte quanto seu elo mais fraco. Com relação à segurança dos dados, esse princípio também é verdadeiro. Um único computador comprometido em uma rede local pode colocar em risco todas as informações enviadas ou armazenadas por aquele prestador de serviço.

É correto pensar que são as falhas de segurança em grandes bancos de dados, por afetarem um grande número de pessoas, que recebem maior atenção midiática e, por isso mesmo, levam a melhoramentos nos mecanismos de segurança e proteção de integridade e confidencialidade desses bancos de dados. Assim, se os organismos que mantêm grandes bancos de dados de RES têm a obrigação – seja por força de norma ou por pressão econômica – de protegerem seus dados, para os cirurgiões-dentistas e médicos em clínicas e consultórios, pelo fato de não formarem grandes bancos de dados de S-RES, o possível vazamento de informações não é objeto de muita preocupação e não tem recebido a devida atenção. Todavia, de acordo com pesquisa realizada por Johnson (2009), verificou-se que informação de saúde, que deveria permanecer protegida, é facilmente encontrada em redes de compartilhamento de arquivos *peer-to-peer*, como por exemplo *bit torrent*, *kazaa* e *e-donkey*, o que demanda atenção imediata para a conscientização dos usuários sobre o perigo de utilização de *software* de compartilhamento de dados, em computadores que servem a múltiplos propósitos, em pequenas clínicas e consultórios, uma vez que seria possível a um usuário remoto, sem direitos sobre as informações, coligir os dados de saúde existentes nos computadores de diversos prestadores de serviços.

Não se deve deixar de levar em consideração, neste ponto, que muitas vezes

os computadores que servem, em consultórios odontológicos, para armazenamento dos prontuários de pacientes e para efetuar a troca de informações nos moldes do TISS servem também para outros fins, sem relação com a prática odontológica. Seja pela praticidade, seja pelo custo ou por outras razões, esses computadores também são utilizados para verificação de e-mails, navegação pelos mais diversos sítios de internet e troca de mensagens instantâneas. Todas essas atividades, se realizadas em computadores que não contam com mecanismos de proteção adequados, como *firewalls* e antivírus, representam um risco de perda ou vazamento de dados devido à potencial contaminação por software malicioso, que pode se apropriar e transmitir informação privilegiada a terceiros.

Temos, portanto, que a legislação estruturante da TISS e os requisitos de segurança por ela propostos e recomendados, apesar de cobrirem com certa eficácia as necessidades de segurança *na troca e armazenamento de dados pelas operadoras*, deixam de levar em consideração as condições diferenciadas em que se encontram os prestadores de serviço, como os cirurgiões-dentistas, em seus consultórios. A ausência de recomendações específicas aos prestadores quanto à necessidade de ações para salvaguardar a característica de segredo e privacidade leva a uma falsa sensação de segurança, expondo boa parte dos 52 milhões de beneficiários de planos de saúde aos riscos decorrentes da divulgação de seus dados pessoais e de saúde. Essa ausência de atenção e orientação direcionada especificamente ao prestador de serviço consiste em um enorme risco em um sistema de troca de informações de saúde e é, ademais, injustificável por existir uma série de recomendações de segurança disponibilizadas pelo Comitê Gestor da Internet no Brasil e que foram, neste momento, por nós adaptadas para uso facilitado do cirurgião-dentista em seu consultório odontológico (Anexo A).

5.2 Das informações enviadas pelas operadoras à ANS

Outro problema que é possível verificar reside no fato de que a própria ANS não deixa claro em que consiste, exatamente, o conjunto de informações sobre os usuários que as operadoras devem enviar nem, tampouco, quais são as medidas de segurança a que estes dados estão sujeitos.

Enquanto a lei 9656/98 estabelece que as operadoras são obrigadas a fornecer, periodicamente, à ANS as informações e estatísticas relativas a suas atividades, em especial as que permitam a identificação dos consumidores e seus dependentes, a ANS afirma que os dados obtidos com o TISS vão permitir, à ANS, uma avaliação da assistência à saúde de caráter clínico, epidemiológico e administrativo, o que indica que os dados passados pelas operadoras não consistem, apenas, em informações cadastrais sobre os beneficiários, mas, também, em informações identificáveis de cada tratamento realizado (Brasil, 1998, 2005a, 2006b, 2008b).

Em consulta à ANS realizada nos meses de agosto e setembro de 2009, na qual foi questionado quais eram as informações adquiridas e que mecanismos de segurança eram utilizados para garantir o segredo dos dados (com protocolo 173596), não obtivemos resposta.

Não há dúvidas de que a sociedade como um todo deve se mobilizar pela transparência dos órgãos públicos, principalmente quando informação privada é coletada. Se por um lado a ANS afirma que a troca de informações em saúde suplementar veio a facilitar a obtenção de informações para o fim de estudos epidemiológicos de um setor que, há até poucos anos, existia sem qualquer tipo de regulamentação, por outro, deixa de informar quais são as informações

armazenadas e analisadas - e, pior ainda, deixa de esclarecer quais são os mecanismos que protegem essa imensa quantidade de informação. É certo que a utilização de métodos de computação eletrônica agilizam o processamento de dados e, a partir disso, facilitam o estabelecimento de políticas públicas de saúde mais eficazes para atender uma realidade social que é discrepante, contraditória e cruel. Se temos de nos perguntar até que ponto as garantias dadas pelo Estado são confiáveis - uma vez que é possível encontrar, à venda, dados bancários, informações fiscais da maior parte dos brasileiros devido ao vazamento de informações dos bancos de dados da Receita Federal, da Secretaria da Fazenda e do Banco Central do Brasil - não podemos dar as costas ao avanço tecnológico e agir como verdadeiros luditas, em nossa época de paradigmas destruídos. Se não é possível estabelecer mecanismos absolutos de segurança de dados, devemos nos pautar pela sempiterna busca do equilíbrio entre a disponibilização dos dados e a segurança da informação. Não podemos, não devemos, entretanto, permanecer calados, à espera de que um *salvador* decida quais informações devem ou não ser protegidas.

O espírito da democracia é arredo e seu exercício não pode ser feito de braços cruzados.

CONCLUSÕES

6. CONCLUSÕES

Apesar de existirem mecanismos adequados de proteção às informações trocadas previstos na legislação estruturante da Troca de Informações em Saúde Suplementar para o armazenamento das informações nas operadoras e para a troca de dados em si, não é possível afirmar, com absoluta certeza, que os dados encontram-se protegidos em todas as etapas.

O histórico de vazamento de dados sensíveis a partir de bancos de dados governamentais e a ausência de instruções dirigidas, especificamente, aos prestadores de serviço, levam a crer, na verdade, que tanto a manutenção do segredo profissional quanto da privacidade dos pacientes encontram-se em risco com a Troca de Informações em Saúde Suplementar.

REFERÊNCIAS

REFERÊNCIAS ⁵

Aron R. Paz e guerra entre as nações. Brasília: UnB; 1986.

Learning to live with Big Brother, The Economist [periódico online], 2007 set. Disponível em: URL: http://www.economist.com/world/international/displaystory.cfm?story_id=9867324 [2008 jul 01].

Abdalla FTM. Abertura da privacidade e o sigilo do HIV/AIDS nas equipes do programa saúde de família de uma unidade básica de saúde do município de São Paulo [Dissertação] São Paulo: Universidade de São Paulo, Escola de Enfermagem; 2007.

Al-Shahi R, Warlow C. Using patient-identifiable data for observational research and audit. BMJ 2000;321:1031-2.

Almeida M, Muñoz D. O princípio e as razões do segredo médico. Rev IMESC São Paulo 1998 dez (1). Disponível em: URL: <http://www.imesc.sp.gov.br/rev1f.htm> [2008 04 jun].

Ball E, Chadwick DW, Mundy D. Patient privacy in electronic prescription transfer. IEEE JNL 2003(1);2:77-80. Disponível em: URL: <http://ieeexplore.ieee.org/iel5/8013/26759/01193217.pdf?tp=&arnumber=1193217&isnumber=26759> [2008 jun 1].

Bastos CR, Martins IG. Comentários à Constituição do Brasil. São Paulo: Saraiva; 1989.

Béjar H. El ámbito íntimo. Madrid: Alianza Editorial; 1995.

Blevins SA. Who's reading your medical files today? Christian Science Monitor [periódico online], 2008 aug 08. Disponível em: URL: <http://www.csmonitor.com/2008/0826/p09s02-coop.html> [2009 set 9].

Brasil. Código Civil Brasileiro. Lei nº 10.406 de 10 de janeiro de 2002a. Institui o Código Civil. Disponível em: URL: http://planalto.gov.br/ccivil_03/Leis/L3071.htm [5 mai 2009].

Brasil. Conselho Federal de Odontologia. Código de Ética Odontológica. Rio de Janeiro; 2006a. Disponível em: URL: http://www.cfo.org.br/download/pdf/codigo_etica.pdf [2009 jun 1].

Brasil. Constituição da República Federativa do Brasil. 1988. Disponível em: URL: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm [2009 set. 9].

⁵ De acordo com Estilo Vancouver. Abreviatura de periódicos segundo base de dados MEDLINE.

Brasil. Lei nº 9.656 de 03 de junho de 1998. Dispõe sobre os planos e seguros privados de assistência à saúde. Disponível em: URL: http://www.ans.gov.br/portal/site/legislacao/legislacao_integra.asp?id_original=455 [2009 set. 9].

Brasil. Lei nº 9.961 de 28 de janeiro de 2000. Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências. Disponível em: URL: http://www.ans.gov.br/portal/site/legislacao/legislacao_integra.asp?id_original=8 [2009 set. 9].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Caderno de Informações da Saúde Suplementar – Setembro de 2008. Brasília; 2006b. Disponível em: URL: http://www.ans.gov.br/portal/site/informacoesss/iss_publicacoes.asp [2009 out 8].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Exposição de motivos para o estabelecimento de padrão essencial obrigatório para as informações trocadas entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde sobre o atendimento prestado a seus beneficiários e usuários. 2005a Disponível em: URL: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/cp_21_exposicao_motivos.pdf [2008 set 9].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Histórico da Troca de Informações em Saúde Suplementar. Brasília; 2008a. Disponível em: URL: http://www.ans.gov.br/portal/site/_hotsite_tiss/f_materia_15254.htm [2008 jun 01].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Manual de conteúdo e estrutura, Brasília, 2007a. Disponível em: URL: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/Manual_de_Conteúdo_e_Estrutura_PDF_v2110.pdf [2008 jun 01].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Manual TISS - Odontologia. Brasília; 2008b. Disponível em: URL: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/Manual_TISS_odontologia.pdf [2008 jun 01].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Resolução Normativa 21 de 12 de dezembro de 2002b. Disponível em: URL: http://www.ans.gov.br/portal/site/legislacao/legislacao_integra.asp?id=390&id_original=0 [2008 jun 01].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Resolução da Diretoria Colegiada 64 de 10 de abril de 2001. Disponível em: URL: http://www.ans.gov.br/portal/site/legislacao/legislacao_integra.asp?id=137&id_original=0 [2008 jun 01].

Brasil. Ministério da Saúde. Agência Nacional de Saúde Suplementar. Resolução Normativa 114 de 26 de outubro de 2005b. Disponível em: URL: http://www.ans.gov.br/portal/site/_hotsite_tiss/f_materia_21227.htm [2008 jun 01].

Brasil. Ministério da Saúde. ANS. Resolução Normativa 153 de 28 de maio de 2007b. Disponível em: URL: http://www.ans.gov.br/portal/site/_hotsite_tiss/f_materia_21227.htm [2008 jun 01].

Brasil. Ministério da Saúde. Conselho Nacional de Secretários de Saúde. Saúde Suplementar. Brasília; 2007c

Brasil. Ministério da Saúde. Conselho Nacional de Secretários de Saúde. Regulação em saúde. Brasília; 2007d

British Medical Association. Survey of the general public's view on NHS System reform in England. 2007. Disponível em: URL: [http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFnhssystreform2007/\\$FILE/48751Surveynhsreform.pdf](http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFnhssystreform2007/$FILE/48751Surveynhsreform.pdf) [2008 jun 01].

Cheswick WR, Bellovin SM, Rubin AD. Firewalls e segurança na internet – repelindo o hacker ardiloso. 2ª. ed. São Paulo: Bookman; 2003.

Choi YB, Capitan KE, Krause JS, et al. Challenges associated with privacy in Health Care Industry: Implementation of HIPAA and the security rules. J Med Sys 2006;30(1):57-64.

Condon R. Poynter report uncovers culture of insecurity at HMRC, Searchsecurity [periódico online]; 2008, junho. Disponível em: URL: http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1318850,00.html [2009 set 9].

Costa Jr PJ. O direito de estar só: tutela penal da intimidade. 3ª ed. São Paulo: Siciliano Jurídico; 2004.

Dallari SG. A justiça, o direito e os bancos de dados epidemiológicos. Ciência & Saúde Coletiva 2007;12(3):663-41.

Damschroder LJ, Pritts JL, Neblo MA, et al. Patients, privacy and trust: Patients' willingness to allow researchers to access their medical records Soc Sci Med 2007;64:223-35.

Daruge E, Massini N. Direitos profissionais na odontologia. São Paulo: Saraiva; 1978.

Dilthey W. Hermeneutics and the study of history. Princeton: Princeton University Press; 1996.

Eco U. O Pêndulo de Foucault. Rio de Janeiro: Record; 1986.

Ellison C, Schneier B. Ten Risks of PKI: What you're not being told about public key infrastructure. Comp Security J 2000;16(1):1-7.

Garcia PPNS, Cobra CS. Condições de Trabalho e Satisfação de Cirurgiões-

Dentistas Credenciados por Convênios Odontológicos. Rev Odontol UNESP 2004; 33(3):115-22.

Huxley A. Admirável mundo novo. São Paulo: Abril; 1974.

Jabur GH. Liberdade de pensamento e direito à vida privada. São Paulo: RT; 2000.

Johnson ME. Data hemorrhages in the health-care sector In: Financial Cryptography and Data Security. Heidelberg: Springer-Berlin; 2009. Disponível em: URL: <http://www.springerlink.com/content/k8vhh4h7w5157w42/fulltext.pdf> [2009 ago 07].

Krishna R, Kelleher K, Stahlberg E. Patient confidentiality in the research use of clinical medical databases. Am J Public Health 2007;97:654-8.

Kroker M, Berke J, Klessea HJ. Operation Goldesel: Kontonummern von 21 Millionen Bürgern illegal im Umlauf, Wirtschaftswoche [periódico online]; 2008, dezembro, 12. Disponível em: URL: <http://www.wiwo.de/unternehmermaerkte/operation-goldesel-kontonummern-von-21-millionen-buerger-illegal-im-umlauf-380237> [2009 set 9].

Louzã JR. Documentos médicos: aspectos éticos e legais In: Segre M, Cohen C, organizadores. Bioética. São Paulo: Edusp; 1995.

Musetti RA. A hermenêutica jurídica de Hans-Georg Gadamer e o pensamento de São Tomás de Aquino, Revista CEJ, abril 1999. Disponível em: URL: <http://www.cjf.jus.br/revista/numero7/artigo18.htm> [2008 jun 01].

Ortega y Gasset J. Meditação sobre a técnica. Rio de Janeiro: Instituto Liberal; 1981.

Orwell G. 1984. São Paulo: Companhia Editora Nacional; 1972.

Polícia de São Paulo fecha site que vendia dados sigilosos. Folha de São Paulo [periódico online]; 2009, julho, 04. Disponível em: URL: <http://www1.folha.uol.com.br/folha/cotidiano/ult95u590657.shtml> [2009 ago 07].

Robling MR, Hood K, Houston H, et al. Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study. J Med Ethics 2004;30:104-9.

Sacardo DP. Expectativa de privacidade segundo pessoas hospitalizadas e não-hospitalizadas: um estudo bioético [Dissertação]. São Paulo: Universidade de São Paulo, Faculdade de Saúde Pública; 2001.

Sacardo DP, Fortes PAC. Desafios para a preservação da privacidade no contexto da saúde. Bioética 2000;8(2):307-22.

Schneier B. US Medical Privacy law gutted, 2005. Disponível em: URL: http://www.schneier.com/blog/archives/2005/06/us_medical_priv.html [2008 jun 1].

Site reúne dados sigilosos de cidadãos; senhas são vendidas. Uol Notícias [periódico online]; 2009, outubro, 09. Disponível em: URL: <http://noticias.uol.com.br/ultnot/multi/2009/10/08/0402386EC4B94366.jhtm?site-reune-dados-sigilosos-de-cidadaos-senhas-sao-vendidas-0402386EC4B94366> [2009 out 09].

Souza, NTC. Erro médico e sigilo profissional. Jus Navigandi, Teresina, 2005 abr;9(636). Disponível em: URL: <http://jus2.uol.com.br/doutrina/texto.asp?id=6529> [2008 4 jun].

Stanford encyclopedia of philosophy. [enciclopédia online] c2005. Disponível em: URL: <http://plato.stanford.edu/entries/hermeneutics/> [2008 jun 01].

Tonelli MLQ. Hermenêutica Jurídica, Jus Navegandi 2002, agosto. Disponível em: URL: <http://jus2.uol.com.br/doutrina/texto.asp?id=4324> [2008 jun 01].

UCLA Medical Center To Face Sanctions After Patient Data Breaches, CaliforniaHealthLine [periódico online]; 2008, abril, 8. Disponível em: URL: <http://www.californiahealthline.org/Articles/2008/4/8/UCLA-Medical-Center-To-Face-Sanctions-After-Patient-Data-Breaches.aspx> [2009 out 10].

Vieira TM. O direito à privacidade na sociedade da informação. Porto Alegre: Sergio Antonio Fabris Editor; 2007.

ANEXOS

ANEXO A - Checklist de referência para manutenção do segredo profissional em ambientes computacionais

Checklist rápido de referência para manutenção do segredo profissional e da privacidade dos pacientes, baseado no checklist de segurança de dados publicado pela CERT, disponível em <http://cartilha.cert.br/download/>:

Contas e senha

- elabore sempre uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos;
- jamais utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários;
- utilizar uma senha diferente para cada serviço;
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador;
- utilizar o usuário Administrator (ou root) somente quando for estritamente necessário.

Vírus

- instalar e manter atualizado um bom programa antivírus;
- atualizar as assinaturas do antivírus, de preferência diariamente;

- configurar o antivírus para verificar os arquivos obtidos pela Internet, discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e pen drives;
- desabilitar no seu programa leitor de e-mails a auto-execução de arquivos anexados às mensagens;
- não executar ou abrir arquivos recebidos por e-mail ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o arquivo, certifique-se que ele foi verificado pelo programa antivírus;
- utilizar na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou PostScript;
- não utilizar, no caso de arquivos compactados, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.
- manter o sistema operacional e demais softwares sempre atualizados;
- aplicar todas as correções de segurança (patches) disponibilizadas pelos fabricantes, para corrigir eventuais vulnerabilidades existentes nos softwares utilizados;
- instalar um firewall pessoal;
- utilizar pelo menos uma ferramenta anti-spyware e mantê-la sempre atualizada.

Cuidados com os Dados Armazenados em Disco Rígido

É importante ter certos cuidados no armazenamento de dados em um computador. Caso o cirurgião-dentista mantenha informações pessoais ou os prontuários de seus pacientes armazenados no formato digital, devem ser armazenadas em algum formato criptografado. Caso as informações não estejam criptografadas, se você necessitar levar o computador a alguma assistência técnica, por exemplo, seus

dados poderão ser lidos ou copiados por uma pessoa não autorizada.

Estes cuidados são extremamente importantes no caso de notebooks, pois são mais suscetíveis a roubos ou furtos.

Para criptografar estes dados, existem programas que, além de serem utilizados para a criptografia de e-mails, também podem ser utilizados para criptografar arquivos.

Um exemplo seria utilizar um programa que implemente criptografia de chaves pública e privada, como o GnuPG. O arquivo sensível seria criptografado com a sua chave pública e, então, decodificado com a sua chave privada, sempre que fosse necessário.

É importante ressaltar que a segurança deste método de criptografia depende do sigilo da chave privada. A idéia, então, é manter a chave privada em um CD ou outra mídia (como pendrive, disco rígido removível ou externo) e que este não acompanhe o computador, caso seja necessário, por exemplo, enviá-lo para uma assistência técnica.

Outra alternativa é a utilização de um software que criptografe as pastas do computador, evitando o acesso de terceiros aos arquivos de prontuários - que devem ser armazenados nestas pastas.

Também deve-se ter um cuidado especial ao trocar ou vender um computador. Apenas apagar ou formatar um disco rígido não é suficiente para evitar que informações antes armazenadas possam ser recuperadas, sendo, portanto, importante sobrescrever todos os dados do disco rígido, com o uso de software específico.

ANEXO B Resolução Normativa N°. 153, de 28 de maio de 2007 da ANS

Estabelece padrão obrigatório para a troca de informações entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde sobre os eventos de saúde, realizados em beneficiários de plano privado de assistência à saúde e dá outras providências.

A Diretoria Colegiada da Agência Nacional de Saúde Suplementar, no uso das atribuições que lhe conferem o art. 20 da Lei n° 9.656, de 03 de junho de 1998, os incisos XXIV e XXXI do art. 4° e o inciso II do art. 10 da Lei n° 9.961 de 28 de janeiro de 2000, em reunião realizada em 24 de maio de 2007, adotou a seguinte Resolução Normativa e eu, Diretor - Presidente, determino sua publicação:

CAPÍTULO I**Das disposições gerais**

Art. 1° - A presente Resolução estabelece padrão obrigatório para troca de informações em saúde suplementar (TISS) entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde sobre os eventos de saúde realizados em beneficiários de plano privado de assistência à saúde, e mecanismos de proteção à informação em saúde suplementar.

Parágrafo único - Ficam dispensadas da adoção do padrão TISS as operadoras classificadas como administradoras de plano.

Art. 2° - O padrão TISS é dividido em quatro partes: conteúdo e estrutura; representação de conceitos em saúde; segurança; e comunicação.

§ 1° O padrão de conteúdo e estrutura constitui modelo de apresentação dos eventos de saúde realizados no beneficiário, e compreende as informações administrativas e assistenciais necessárias para a autorização e o pagamento dos eventos assistenciais realizados, como as guias e seus anexos, o demonstrativo de pagamento e o demonstrativo de análise de conta médica, assim definidos:

I - Guias: modelo formal e obrigatório de representação e descrição documental do padrão TISS, sobre os eventos de saúde realizada no beneficiário de plano privado de assistência à saúde, e enviado do prestador para a operadora.

- a) guia de consulta;
- b) guia de solicitação e de realização de serviço profissional/serviço auxiliar de diagnóstico e terapia - SP/SADT;
- c) guia de solicitação de internação;
- d) guia de resumo de internação;
- e) guia de honorário individual;
- f) guia de solicitação de tratamento odontológico;
- g) guia de procedimentos odontológicos realizados;
- h) guia de outras despesas;

II - anexos: informações complementares sobre os eventos de

assistência à saúde prestados nos beneficiários, como programas específicos de gerenciamento de cuidados;

III - demonstrativo de pagamento: modelo formal e obrigatório de representação e descrição documental do padrão TISS, sobre o pagamento dos eventos de saúde realizados no beneficiário de plano privado de assistência à saúde, enviado da operadora para o prestador;

IV - demonstrativo de análise de conta médica: modelo formal e obrigatório de representação e descrição documental do padrão TISS, sobre a análise das contas dos eventos de saúde realizados no beneficiário de plano privado de assistência à saúde, enviado da operadora para o prestador.

§ 2º O padrão de representação de conceitos em saúde constitui conjunto padronizado de terminologias, códigos e descrições utilizados no padrão TISS.

§ 3º O padrão de comunicação define os métodos para se estabelecer comunicação entre os sistemas de informação das operadoras de planos privados de assistência à saúde e os sistemas de informação dos prestadores de serviços de saúde e as transações eletrônicas.

§ 4º O padrão de segurança estabelece os requisitos mínimos das proteções administrativas, técnicas e físicas necessárias à garantia da confidencialidade das informações em saúde.

§ 5º Compete à Diretoria de Desenvolvimento Setorial – DIDES definir, por meio de Instrução Normativa, os padrões de que tratam os parágrafos 1º, 2º, 3º e 4º deste artigo.

Art. 2º Os padrões de comunicação seguem a linguagem de marcação de dados XML (Extensible Markup Language).

§ 1º Ficam definidas as seguintes transações eletrônicas:

I - a serem feitas dos prestadores de serviços de saúde para as operadoras de planos privados de assistência à saúde: solicitação de autorização de procedimento, envio de lotes de guias, solicitação de demonstrativo de retorno, solicitação de elegibilidade, solicitação de status da autorização, solicitação de cancelamento de guia e solicitação do status do protocolo; e

II - das operadoras de planos privados de assistência à saúde para os prestadores de serviços de saúde: envio de autorização de procedimento, envio de recibo de lotes de guias, envio do demonstrativo de retorno, resposta à elegibilidade, resposta status de autorização, confirmação cancelamento de guia e envio do status do protocolo.

§ 2º Compete à Diretoria de Desenvolvimento Setorial – DIDES definir, por meio de Instrução Normativa, as estruturas das transações eletrônicas estabelecidas no § 1º deste artigo.

CAPÍTULO II

Do Cronograma para adoção do padrão TISS

Art. 3º O padrão TISS será adotado de forma gradual, observando o determinado nos parágrafos seguintes.

§ 1º Para a implantação do padrão TISS, os prazos serão os previstos nos §§ 2º e 3º do presente artigo, variando de acordo com o tipo de prestador de serviços, assim agrupados:

I - grupo 1:

a) hospitais gerais - hospital destinado à prestação de atendimento nas

especialidades básicas, por especialistas e/ou outras especialidades médicas. Pode dispor de serviço de urgência/emergência;

b) hospitais especializados - hospital destinado à prestação de assistência à saúde em uma única especialidade/área. Pode dispor de serviço de urgência/emergência e SADT;

c) hospitais/dia-isolado - unidades especializadas no atendimento de curta duração com caráter intermediário entre a assistência ambulatorial e a internação;

d) pronto socorro especializado - unidade destinada à prestação de assistência em uma ou mais especialidades, a pacientes com ou sem risco de vida, cujos agravos necessitam de atendimento imediato; e

e) pronto socorro geral - unidade destinada à prestação de assistência a pacientes com ou sem risco de vida, cujos agravos necessitam de atendimento imediato. Podendo ter ou não internação;

f) clínica especializada/ambulatório de especialidade;

g) unidade de apoio à diagnose e terapia (SADT isolado);

h) unidade móvel de nível pré-hospitalar - urgência/emergência;

i) unidade móvel fluvial;

j) unidade móvel terrestre; e

k) policlínica.

II - grupo 2:

a) consultório médico isolado;

b) profissionais de saúde ou pessoas jurídicas que prestam serviços em consultórios médicos;

III - grupo 3:

a) clínica radiológica em odontologia;

b) consultório odontológico isolado; e

c) odontólogo ou pessoa jurídica da área odontológica que preste serviços em consultórios.

§ 2º Os prazos para a implantação do padrão de conteúdo e estrutura – guias, demonstrativo de análise de conta médica e demonstrativos de pagamento – e do padrão de representação dos conceitos de saúde – entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde – agrupados conforme estabelecido no § 1º deste artigo, são:

I - entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde do grupo 1: até o dia 31 de maio de 2007;

II - entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde do grupo 2: até o dia do 31 de maio de 2007;

III - entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde do Grupo 3: até o dia 31 de maio de 2008.

§ 3º Os prazos para a implantação dos padrões TISS de comunicação e de segurança – entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde – agrupados conforme estabelecido no § 1º deste artigo, são:

I - entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde do grupo 1: até o dia 31 de maio de 2007;

II - entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde do grupo 2: até o dia do 30 de novembro de

2008;

III - entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde do Grupo 3: até o dia 30 de novembro de 2008.

CAPÍTULO III

DO ACOMPANHAMENTO DA IMPLANTAÇÃO DO PADRÃO TISS

Art. 4º A partir de 1º de setembro de 2007, as operadoras encaminharão eletronicamente para a ANS os modelos por elas adotados das guias e dos demonstrativos previstos nos incisos do § 1º do artigo 2º desta RN, bem como outras informações sobre a implantação do padrão TISS, na forma e nos prazos a serem definidos em Resolução Normativa da ANS.

CAPÍTULO IV

DO COMITÊ DE PADRONIZAÇÃO DAS INFORMAÇÕES EM SAÚDE SUPLEMENTAR

Art. 5º Fica mantido o Comitê de Padronização das Informações em Saúde Suplementar - COPISS, de caráter consultivo, criado pela Resolução Normativa nº 114, de 26 de outubro de 2005, sob coordenação da Diretoria de Desenvolvimento Setorial da ANS, com as seguintes atribuições:

I - supervisionar, coordenar, estabelecer prioridades e propor modificações e melhorias no padrão TISS;

II - estabelecer e promover metodologia de divulgação das informações do padrão TISS;

III - revisar e aprovar termos e classificações utilizados no padrão TISS;

IV - promover, fomentar e recomendar estudos relacionados à padronização das informações em saúde suplementar bem como para a troca eletrônica de informações em saúde suplementar, baseados nos padrões nacionais e internacionais;

V - identificar, propor e coordenar modificações necessárias aos sistemas de informação da saúde suplementar, sob coordenação da ANS, para adequação aos padrões consensuados e aos sistemas de informações de saúde do MS.

VI - propor padrões e metodologias para proteger e melhorar a confidencialidade, disponibilidade e integridade da informação em saúde suplementar, bem como as boas práticas para gerenciamento seguro da informação em saúde.

§ 1º O Comitê é constituído por representantes da Agência Nacional de Saúde Suplementar, do Ministério da Saúde, das operadoras de planos privados de assistência à saúde, dos prestadores de serviços de saúde, das instituições de ensino e pesquisa, de representações de usuários, e de eventuais convidados da coordenação do Comitê de Padronização das Informações em Saúde Suplementar.

§ 2º Compete à DIDES, por meio de Instrução Normativa, indicar os representantes do Comitê de Padronização das Informações em Saúde Suplementar, determinar a periodicidade das reuniões e definir o modelo de solicitação de modificação do padrão TISS (SOP-TISS).

§ 3º Qualquer interessado na padronização da troca de informações em saúde, sem representatividade no Comitê de Padronização, poderá encaminhar sugestões para apreciação mediante preenchimento do modelo SOP-TISS.

§ 4º Antes de 360 dias a contar da data de publicação desta Resolução, ficam vedadas modificações no padrão TISS publicado, salvo por motivo relevante.

§ 5º As modificações serão avaliadas sob critérios que visem:

I - redução de custos administrativos;

II - aumento da eficiência, eficácia e efetividade da atenção a saúde;

III - integração dos sistemas de informação em saúde adotados pela Agência Nacional de Saúde Suplementar e pelo Ministério da Saúde, ou demais órgãos/autarquias relacionadas com os serviços de saúde; e

IV - harmonização com os padrões nacionais e internacionais, elaborados pelas organizações produtoras de padrão de informação em saúde.

CAPÍTULO V

DA REQUISIÇÃO DE INFORMAÇÕES PELA ANS

Art. 6º Toda e qualquer informação relativa a eventos de saúde, requisitada pela ANS, a partir da publicação desta Resolução, deverá ser realizada e prestada conforme previsto no padrão TISS.

§ 1º Caso a informação necessária não esteja prevista no padrão, deverá ser nele incluída através da metodologia descrita no artigo 6º desta Resolução.

§ 2º Ficam mantidas e preservadas as rotinas sistemáticas e contínuas de coleta e transmissão de dados entre as operadoras de planos privados de assistência à saúde e a ANS, bem como os requerimentos de informação, de caráter excepcional.

§ 3º O envio das informações requisitadas pela ANS não exime as operadoras nem os prestadores da obrigação de apresentar documentação comprobatória da veracidade das informações prestadas, bem como de quaisquer outros documentos e informações que a ANS, nos limites de sua competência, vier a requisitar.

CAPÍTULO VI

DA SEGURANÇA E DA PRIVACIDADE

Art. 7º As operadoras de planos privados de assistência à saúde e os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial a toda informação identificada individualmente, conforme normas técnicas estabelecidas na Resolução CFM nº 1639 de 10 de julho de 2002, e na RN nº 21 de 12 de dezembro de 2002, e na RDC nº 64 de 10 de abril de 2001 ambas da ANS.

§ 1º As operadoras de planos privados de assistência à saúde e os prestadores de serviços de saúde que optem pela forma de comunicação através da rede Internet, inclusive as que optem pela utilização de empresas intermediadoras prestadoras de serviços de conectividade, devem obrigatoriamente adotar os requisitos de segurança do Nível de Garantia de Segurança 1 (NGS-1), descritos no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES), publicado na página da Sociedade Brasileira de Informação em Saúde - SBIS, e do Conselho Federal de Medicina - CFM, conforme norma NBR ISO/IEC 17799 - Código de Prática para a Gestão da Segurança da Informação.

§ 2º Para as operadoras de planos privados de assistência à saúde e prestadores de serviços médico-hospitalares que utilizarem Webservices,

recomenda-se a utilização do Nível de Garantia de Segurança 2 (NGS-2).

Art. 8º Para as transmissões remotas de dados identificados, os sistemas deverão possuir um certificado digital de aplicação única emitido por uma Autoridade Certificadora (AC) credenciada pelo Instituto Nacional de Tecnologia da Informação – ITI, responsável pela AC Raiz da estrutura da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, a fim de garantir a identidade do sistema.

§ 1º O certificado digital deve ter como um de seus atributos o Cadastro de Pessoa Física - CPF ou o Cadastro Nacional da Pessoa Jurídica - CNPJ do prestador.

§ 2º No caso de pessoa jurídica em que trabalhem vários prestadores pessoa física, todos os dados poderão trafegar sob o certificado da pessoa jurídica, devendo as operadoras manter registro do vínculo entre esses prestadores.

CAPÍTULO VII DA COMUNICAÇÃO

Art. 9. As operadoras de planos privados de assistência à saúde e os prestadores de serviços de saúde devem adotar uma das formas previstas neste Capítulo de comunicação do padrão TISS para a troca de informações sobre os eventos assistenciais realizados aos beneficiários de planos de saúde.

Art. 10. As operadoras de planos privados de assistência à saúde devem atender a requisições através da Internet, adotando preferencialmente a tecnologia de Webservices padronizada por Instrução Normativa da DIDES para transações realizadas em tempo real.

§ 1º Adotando ou não tecnologia Webservices, as operadoras de planos privados de assistência à saúde podem disponibilizar para suas redes prestadoras portais de acesso aos serviços do padrão TISS ou outras formas de comunicação não proprietária e obrigatoriamente devem possibilitar o envio dos arquivos no padrão de comunicação através de upload/download nesses portais.

§ 2º As operadoras de planos privados de assistência à saúde podem submeter dados não padronizados para que empresas intermediadoras de prestação de serviços de conectividade os processem em mensagens no padrão TISS e transmitam para os prestadores vinculados/credenciados, ou podem utilizar empresas intermediadoras prestadoras de serviços de conectividade para receber mensagens no padrão TISS dos prestadores vinculados/credenciados, desde que sejam observados os requisitos de segurança estabelecidos nesta norma. Os mesmos procedimentos podem ser adotados pelos prestadores de serviços em saúde.

Art. 11. Os prestadores de serviços de saúde vinculados/credenciados a operadoras de planos privados de assistência à saúde têm a prerrogativa de escolher a forma de comunicação que melhor lhes convier sem nenhum tipo de imposição tecnológica ou comercial de outra parte, desde que respeitados os prazos e os padrões estabelecidos nesta Resolução.

Art. 12. Qualquer tecnologia poderá ser utilizada desde que consiga atender na íntegra as normas e todos os padrões do TISS, e que seja não proprietária,

a fim de facilitar a utilização por todos os atores envolvidos.

Art. 13. A interrupção do serviço de troca eletrônica de informações

entre prestadores de serviços de saúde e operadoras de planos privados de assistência à saúde deve ser solucionada em até 48 (quarenta e oito) horas, salvo em caso fortuito ou de força maior devidamente justificado.

§ 1º Enquanto perdurar a interrupção de que trata o caput, as operadoras e os prestadores deverão utilizar o padrão de conteúdo e estrutura como forma contingencial de troca de informações sobre os eventos assistenciais realizados aos beneficiários de planos de saúde.

§ 2º As operadoras de plano de saúde privado e os prestadores de serviços afetados pela interrupção de que trata o caput devem manter registro com histórico que demonstre as ações tomadas e o respectivo tempo de implementação para o restabelecimento da troca de mensagens eletrônicas.

§ 3º A interrupção de que trata o caput deste artigo não pode importar em descontinuidade no atendimento assistencial ao beneficiário de plano de saúde privado, devendo as entidades adotar formas alternativas de comunicação para a autorização do atendimento assistencial.

CAPÍTULO VIII

DAS PENALIDADES

Art. 14. A inobservância da obrigação prevista no artigo 5º desta Resolução configurará a infração administrativa prevista no artigo 34 da RN no 124, de 30 de março de 2006.

Art. 15. A inobservância dos padrões previstos nesta Resolução e nas Instruções Normativas a que se referem o § 5º do art. 2º e o § 2º do art. 3º nos prazos limites para implantação do padrão TISS estabelecidos no art. 4º configurará a infração administrativa prevista no artigo 44 da RN no 124, de 30 de março de 2006.

Art. 16. A denúncia de que trata o artigo 29 da Lei no 9.656, de 3 de junho de 1998, quando relativa à infração prevista no artigo acima, será preliminarmente apurada e instruída pela Gerência-Geral de Integração com o SUS, seguindo os procedimentos de representação de que trata o artigo 8º da RN no 48, de 19 de setembro de 2006, alterado pela RN nº 142, de 21 de dezembro de 2006.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 17. Revogam-se as Resoluções Normativas no 114, de 26 de outubro de 2005, 127, de 11 de maio de 2006, 135, de 28 de setembro de 2006, e 138, de 21 de novembro de 2006.

Art. 18. Esta Resolução Normativa entra em vigor na data de sua publicação.

FAUSTO PEREIRA DOS SANTOS

Diretor-Presidente