SIGILO DAS INFORMAÇÕES

Sergio Miranda Freire[1]

Resumo

A moderna sociedade da informação utiliza um conjunto muito amplo de informações de indivíduos e instituições para propiciar atendimento à saúde de pacientes, planejar a alocação de recursos, regular as ações de operadoras de planos de saúde, planejar a gestão de serviços de saúde, etc. Estas informações são obtidas a partir de formulários em papel, bancos de dados isolados e por meio de vínculos entre bancos de dados pertencentes a instituições diferentes. Por outro lado, esta ampla disponibilidade de dados propicia o risco de acesso e uso indevido e de quebra de privacidade de indivíduos e instituições. Este trabalho realiza uma revisão parcial da legislação nacional e internacional sobre o tema de sigilo das informações na área de saúde. A legislação brasileira tem refletido, especialmente nos último anos, uma preocupação com esta questão , o que tem propiciado a publicação de diversos decretos e resoluções, e a criação de um grupo de trabalho para tratar da certificação de sistemas de prontuário eletrônico. Por outro lado é necessário o estabelecimento de uma legislação que consolide as diversas normas publicadas em uma legislação específica para a área da saúde e que leve em conta outros aspectos até então não contemplados ou não claramente definidos. O trabalho apresenta recomendações para o estabelecimento dessa legislação.

I) INTRODUÇÃO

O sistema de saúde do Brasil envolve uma rede de instituições públicas e privadas e de profissionais: Ministério da Saúde, secretarias estaduais e municipais, postos de saúde, hospitais, clínicas, laboratórios, operadoras de planos de saúde, agências reguladoras, associações profissionais, sociedades científicas, instituições acadêmicas,

[1] Professor Adjunto da Disciplina de Informática Médica da Universidade do Estado do Rio de Janeiro

consultórios médicos, etc. O ser humano é o foco principal desta rede como paciente e como objeto de ação de promoção à saúde e prevenção de doenças. No papel de paciente, cada episódio de contato com algum nó da rede de saúde gera dados que são registrados de alguma forma: prontuário mantido por instituições ou profissionais de saúde, cadastros e histórico de exames e seus resultados em laboratórios, etc. Estes registros são fundamentais para o acompanhamento da assistência prestada a pacientes e exercem outras funções que serão consideradas mais adiante.

No âmbito de cada instituição de saúde, diversos registros são necessários para gerir as diversas atividades que garantem a assistência à saúde e permitem novos investimentos: orçamento e contabilidade, faturamento, planejamento, avaliação do perfil epidemiológico, controle de infecção hospitalar, histórico e cadastro de equipamentos, gerência de recursos humanos, patrimônio, serviço de documentação médica, registro de efeitos adversos de medicamentos e tratamentos, autorização de procedimentos, etc. Uma operadora de planos de saúde, além das atividades típicas de uma empresa moderna, também mantêm cadastros de seus beneficiários e das instituições prestadoras de assistência, além de registros de todos os desembolsos e receitas obtidas.

Os gestores da saúde pública, principalmente os órgãos públicos do Sistema Único de Saúde, garantem a oferta de serviços de saúde nas unidades públicas por meio de orçamento, ou ressarcimento através de AIHs (Autorização de Internação Hospitalar), APACs (Autorização de Procedimentos de Alta Complexidade), e BPAs (Boletim de Produção Ambulatorial). Esses dados são enviados mensalmente pelas unidades de saúde aos respectivos gestores, constituindo de dados de pacientes individuais (APACs e AIHs) e informações agregados (BPAs). Por outro lado, dados de alta qualidade são necessários para que cuidados clínicos mais efetivos possam ser proporcionados; a qualidade e custo-efetividade de serviços de saúde possam ser avaliadas; fraudes e abusos no sistema de saúde possam ser monitorizados; os serviços de saúde proporcionados para populações carentes e os padrões de morbidade e mortalidade entre aquelas populações possam ser acompanhados e avaliados, e outros.

O avanço sobre o conhecimento das causas, prognóstico, prevenção e tratamento de doenças requer a realização de pesquisas que se utilizam de dados de indivíduos ou dados agregados, dependendo da natureza do estudo. Esses dados podem ser obtidos de bases secundárias, registros já existentes ou serem especialmente coletados para a realização do estudo.

Finalmente, no âmbito da regulação das atividades das operadoras de planos de assistência suplementar à saúde, a Agência Nacional de Saúde Suplementar precisa lidar com informações provenientes de diversas fontes: prestadores de assistência à saúde, operadoras de planos de saúde, sistemas de informação do SUS, beneficiários de planos de saúde, etc. Os consumidores também necessitam de informações para tomar decisões referentes a planos e prestadores de atenção à saúde.

Todos os exemplos apresentados acima ilustram, de maneira clara, o grande volume de informações utilizadas em cada nó do sistema de saúde e o fluxo dessas informações entre os diversos nós da rede. A atual infra-estrutura proporcionada pela tecnologia da informação oferece condições que facilitam uma eficiente coleta e uso dos dados. As facilidades dessa infra-estrutura podem incluir: 1) registro eletrônico do paciente que contém registros longitudinais do nascimento à morte dos pacientes; 2) sistemas de informação que capacitam uma coleta, uso e reconfiguração mais sistemática e abrangente da informação em saúde; 3) cartão eletrônico que habilita que os dados do paciente sejam registrados e acessados em um cartão emitido para o paciente; 4) identificadores únicos do paciente que estabelecem um vínculo com várias bases de dados na atenção à saúde e com bases não relacionadas à saúde (créditos, bancos, registros militares). Registros únicos para instituições podem exercer funções semelhantes; 5) redes internas projetadas para compartilhar informações entre organizações afiliadas que proporcionam serviços médicos, serviços de reembolso, revisão de qualidade, etc; 6) redes públicas, como a Internet, que permitem a integração de informações sobre a atenção à saúde e de outros tipos em diversas instituições espalhadas geograficamente (GOSTIN, 1997). A área de saúde tem sido caracterizada por um lento processo de incorporação das modernas tecnologias da informação. Entretanto, a complexidade das atividades da área de saúde e o reconhecimento dos ganhos de qualidade e controle obtidos com os

sistemas de informação têm levado à informatização, muitas vezes de forma mal planejada, das atividades. O aprofundamento da informatização e integração dos sistemas de informação no sistema de saúde do país tem o potencial de produzir um salto de qualidade no gerenciamento do sistema como um todo e na atenção à saúde da população.

Um exemplo claro deste potencial é o prontuário eletrônico do paciente (PEP), o qual pode ser conceituado como o conjunto de informações sobre o estado e cuidados de saúde ao longo da vida de um paciente armazenadas eletronicamente e pode incluir, além das informações resultantes da atenção ao paciente, outras funções não disponíveis no prontuário em papel: alertas e lembretes, módulo de crítica da prescrição médica, ligações com bases de conhecimentos para apoio à decisão, incorporação de protocolos clínicos, interfaces adaptadas pelo usuário, integração com os laboratórios e farmácia, módulo que permite a consulta on-line a bases de trabalhos científicos, etc (DICK et al, 1997, SHORTLIFFE, 1998). Além de seu uso intra-institucional, o PEP pode ser acessado fora dos limites institucionais, permitindo a integração de dados de pacientes dispersos geograficamente.

A par de todos os benefícios citados acima, resultantes da transmissão e utilização judiciosas da informação, existem os riscos associados à perda de privacidade e confidencialidade e o uso indevido de informações. A coleta sistemática de um conjunto amplo de dados pessoais e de instituições apresenta um compromisso substancial em relação à perda da privacidade pessoal e o risco de informações de empresas serem observadas pelos concorrentes, por exemplo.

Os registros de pacientes podem conter uma vasta quantidade de informações pessoais: 1) informações demográficas como idade, sexo, raça, e ocupação; 2) informações financeiras, como renda e tipo de emprego; 3) informações sobre disfunções físicas e/ou cognitivas, necessidades médicas especiais; 4) informações médicas sobre diagnóstico, tratamento, e história da doença (incluindo doença mental, dependência de drogas ou álcool, AIDS, e doenças sexualmente transmissíveis); 5) informações genômicas, e doenças relacionadas à genética; 6) informações pessoais e sociais, tais como orientação sexual, status familiar,

relacionamentos sexuais; e 7) informações sobre o fato de haver sido vítima ou causador de comportamento violento, tais como estupro, abuso de crianças, ou ferimento à bala. As informações disponíveis são freqüentemente suficientes para proporcionar um perfil detalhado da pessoa.

Do lado das operadoras de planos de saúde, uma série de dados institucionais e dos beneficiários tem de ser transmitida para agências reguladoras como parte do processo de regulação e por exigência de regulamentos. Em um regime de concorrência, esses dados não devem estar normalmente disponíveis a seus concorrentes.

Dessa forma, um compromisso tem que ser atingido entre a necessidade assistencial, gerencial, social e científica que requer o acesso e a disponibilidade de informações nos locais em que elas serão utilizadas e a necessidade de se manter a privacidade e a confidencialidade dessas mesmas informações. Mesmo há pouco tempo atrás, quando o nível de informatização era baixo, essa era uma questão que surgia sempre que a utilização de informações de indivíduos e instituições era necessária. Porém, a tecnologia atual desperta temores em um grau bem maior pelo fato de que o vínculo entre diversas bases de dados podem ser estabelecidos, a velocidade de acesso é muito rápida, as barreiras geográficas ou institucionais são mais virtuais do que físicas. Nesse ambiente, o potencial para a invasão da privacidade e uso inescrupuloso das informações não deve ser desprezado e medidas devem ser tomadas para disciplinar a disponibilidade e o acesso e garantir a segurança, privacidade e confidencialidade das informações.

O objetivo deste trabalho é apresentar uma revisão da legislação sobre o sigilo das informações na área de saúde e realizar uma discussão sobre a mesma. Esse trabalho está estruturado em seções, sendo que a seção II descreve uma revisão da legislação nacional e internacional a respeito do assunto. A seção III aborda alguns aspectos envolvendo a segurança de sistemas de informação. A seção IV faz uma análise crítica, dentro do contexto brasileiro, do que foi apresentado nas seções anteriores e a última seção sugere algumas recomendações para o encaminhamento futuro dessa

questão. O Apêndice apresenta um conjunto de termos técnicos para facilitar a compreensão do texto que se segue.

LEGISLAÇÃO

Esta seção está dividida em duas partes, a primeira englobando parcialmente a legislação nacional e a segunda parte a legislação internacional. A legislação nacional consultada foi obtida por meio de entrevistas com advogados funcionários da Agência Nacional de Saúde, e busca na internet; por meio das páginas do Ministério da Saúde, Agência Nacional de Saúde Suplementar, Conselho Federal de Medicina e da Casa Civil da Presidência da República. A legislação internacional se baseou em um trabalho de revisão do Instituto de Pesquisa em Saúde do Canadá (CIHR, 2001).

II.1) LEGISLAÇÃO NACIONAL

II.1.1) LEGISLAÇÃO FEDERAL

A constituição federal (BRASIL, 1988), em seu Art. 5º, assegura a todos os brasileiros a inviolabilidade do direito à segurança, abrangendo entre outros os seguintes itens:

1) é inviolável o sigilo de dados;
2) é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
3) são 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;
4) todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
5) conceder-se-á "habeas-data":

- para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
- para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

O artigo 21 estabelece que a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

No artigo 196, a constituição estabelece que "A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação".

Deste modo, fica consubstanciada na constituição os direitos individuais à privacidade, mas prevê situações onde o interesse público, na área de saúde, em função de *políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação*, ou por necessidade de *exercício profissional*, pode relativizar o sigilo absoluto de dados.

O Código Civil (BRASIL, 2002a) mantém o espírito da constituição, em seus artigos 20 e 21:

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.

Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

O Código Penal (Brasil, 1940), nos artigos 153 e 154, estabelece penas para a violação de sigilo de documentos ou de informações contidas em sistemas de informação, e violação do sigilo profissional:

Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

§ 1º - Somente se procede mediante representação. (Parágrafo único renumerado pela Lei nº 9.983, de 14.7.2000)

§ 1º- A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Parágrafo acrescentado pela Lei nº 9.983, de 14.7.2000)

Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

§ 2o Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada. (Parágrafo acrescentado pela Lei nº 9.983, de 14.7.2000)

Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Parágrafo único - Somente se procede mediante representação.

Os artigos 347, 363 e 406 do Código de Processo Civil (Brasil, 1973) dizem respeito, entre outros itens, ao depoimento e apresentação de documentos nas situações onde o depoente apresenta o dever profissional de manter sigilo:

Art. 347. A parte não é obrigada a depor de fatos:

II - a cujo respeito, por estado ou profissão, deva guardar sigilo.

Parágrafo único. Esta disposição não se aplica às ações de filiação, de desquite e de anulação de casamento.

Art. 363. A parte e o terceiro se escusam de exibir, em juízo, o documento ou a coisa: (Redação dada pela Lei nº 5.925, de 1º.10.1973)

IV - se a exibição acarretar a divulgação de fatos, a cujo respeito, por estado ou profissão, devam guardar segredo; (Redação dada pela Lei nº 5.925, de 1º.10.1973)
Parágrafo único. Se os motivos de que tratam os ns. I a V disserem respeito só a uma parte do conteúdo do documento, da outra se extrairá uma suma para ser apresentada em juízo. (Redação dada pela Lei nº 5.925, de 1º.10.1973)
Art. 406. A testemunha não é obrigada a depor de fatos:
II - a cujo respeito, por estado ou profissão, deva guardar sigilo.

O Código de Proteção e Defesa do Consumidor (BRASIL, 1990), em seu artigo 6º, garante como direitos básicos dos consumidores, entre outros, a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem.

No artigo 43, o código assegura ao consumidor o acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Esses cadastros não podem conter informações negativas referentes a período superior a 5 (cinco) anos, e o consumidor pode realizar correções em seus cadastros. Os bancos de dados e cadastros relativos aos consumidores são considerados entidades de caráter público.

No artigo 44, o mesmo código estabelece que "Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentais contra fornecedores de produtos e serviços, devendo divulgá-los pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor", sendo facultado o acesso a esses cadastros para consulta.

O Código de Proteção e Defesa do Consumidor; portanto, dá o direito de acesso aos pacientes aos seus dados nos prontuários e solicitação de correções dos dados que o mesmo julgar incorretas. O mesmo se aplica aos cadastros de beneficiários em operadoras de planos de saúde e outros.

O Decreto 4.553 (BRASIL, 2002b), de 27 de dezembro de 2002, dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, **no âmbito da Administração Pública Federal**. Este decreto considera sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. Este decreto explicita um importante princípio que determina que "**o acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer**". Este decreto estabelece, entre outras, normas para a classificação de dados ou informações segundo o grau de sigilo, os procedimentos para a classificação de documentos, a marcação, a expedição, o registro, a tramitação, a guarda, a reprodução e o acesso a documentos sigilosos. Ele também estabelece as normas que os sistemas de informação que lidam com informações sigilosas devem obedecer.

O decreto 4553, apesar de se restringir ao âmbito da administração pública federal, estabelece uma série de normas que pode orientar procedimentos semelhantes em outras áreas da administração pública e privada.

A Medida Provisória 2.200-2 (BRASIL, 1001), de 24 de agosto de 2001, institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em meio eletrônico, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. Esta medida considera documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos que ela trata. As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiras em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1^{o} de janeiro de 1916 - Código Civil. O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem

certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

II.1.2) NORMAS E REGULAMENTOS DA AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR

A Agência Nacional de Saúde Suplementar – ANS foi criada em 2000, com a finalidade institucional de *promover a defesa do interesse público na assistência suplementar à saúde, regulando as operadoras setoriais, inclusive quanto às suas relações com prestadores e consumidores, contribuindo para o desenvolvimento das ações de saúde no País*. A criação da ANS resultou de um longo processo e de um conjunto de ações do Governo Federal no sentido de regular o campo da assistência suplementar à saúde (VIANA et al, 2001)

A Lei nº 9.961, de 28 de janeiro de 2000 (BRASIL, 2000) cria a ANS e define a sua área de competência. Para cumprir com seus objetivos, a ANS necessita de uma série de dados e informações das operadoras. Os incisos XVIII e XXXI, e o parágrafo 1º do Art. 4º da referida lei, dá poderes à ANS de solicitar essas informações, conforme apresentado abaixo:

Art. 4º Compete à ANS:

XVIII - expedir normas e padrões para o envio de informações de natureza econômico-financeira pelas operadoras, com vistas à homologação de reajustes e revisões;

XXXI - requisitar o fornecimento de informações às operadoras de planos privados de assistência à saúde, bem como da rede prestadora de serviços a elas credenciadas;

§ 1º A recusa, a omissão, a falsidade ou o retardamento injustificado de informações ou documentos solicitados pela ANS constitui infração punível com multa diária de R$ 5.000,00 (cinco mil reais), podendo ser aumentada em até vinte vezes, se necessário, para garantir a sua eficácia em razão da situação econômica da operadora ou prestadora de serviços.

Consoante as suas atribuições, a ANS vem emitindo uma série de resoluções que visa a normatizar e padronizar o envio de informações das operadoras de planos

de assistência à saúde. Dependendo da resolução ou da natureza das informações, o envio das mesmas por parte das operadoras pode ser através de meio magnético, pela internet, ou em papel, em caso de documentos. A ANS oferece uma área segura na BBS do DATASUS para a transmissão das informações. A resolução nº 3 (ANS, 2000a) aprova normas de fornecimento de informações para cadastros de beneficiários, os quais devem ser transferidos exclusivamente por meio magnético. Este é compactado e criptografado com senha e é transmitido para a BBS do DATASUS em área reservada. A resolução nº 4 (ANS, 2000b) dispõe sobre alteração de rotina do registro provisório de produtos. A resolução nº 5 (ANS, 2000c) aprova normas sobre os procedimentos administrativos para requerimento de concessão de registro provisório das operadoras de Planos Privados de Assistência à Saúde. A resolução 22 (ANS, 2000d) cria instrumento para acompanhamento econômico-financeiro das Operadoras. A resolução nº 23 (ANS, 2000e) altera a Resolução RDC nº 10, de 3 de março de 2000, institui ficha de Compensação, e estabelece padronização para o envio das informações mencionadas na resolução. A resolução nº 24 (ANS, 2000f) dispõe sobre a aplicação de penalidades às operadoras de planos privados de assistência à saúde. As resoluções nº 29 (ANS, 2000g) e nº 66 (ANS, 2001b) estabelecem normas para reajuste das contraprestações pecuniárias dos planos e produtos privados de assistência suplementar à saúde. A resolução 64 (ANS, 2001a) dispõe sobre a designação de médico responsável pelo fluxo de informações relativas à assistência médica prestada aos consumidores de planos privados de assistência à saúde.

Acompanhando a tendência na utilização de sistemas de informação, a ANS emitiu a resolução nº 85 (ANS, 2001c), que institui o Sistema de Informações de Produtos – SIP para o acompanhamento da assistência prestada aos beneficiários de planos privados de assistência à saúde.

Finalmente a resolução normativa 21 (ANS, 2002) dispõe sobre o sigilo das informações dos pacientes por parte das operadoras de planos privados de assistência à saúde:

Art. 1º 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, observado o disposto na Resolução - RDC nº 64, de 10 de abril de 2001, quando acompanhadas de dados que possibilitem a sua individualização, não podendo as mesmas serem divulgadas ou fornecidas a terceiros, salvo em casos expressamente previstos na legislação:
Art. 2º O art. 5º da Resolução - RDC nº 24, de 13 de junho de 2000, passa a vigorar acrescido dos seguintes dispositivos:
"XIV - divulgar ou fornecer a terceiros não envolvidos na prestação de serviços assistenciais, informação sobre as condições de saúde dos consumidores, contendo dados de identificação, sem a anuência expressa dos mesmos, salvo em casos autorizados pela legislação"; e
"XV - divulgar ou fornecer a terceiros não envolvidos na prestação de serviços assistenciais, as informações contidas na declaração de saúde preenchida pelo consumidor por ocasião da contratação de plano de assistência à saúde."

O conjunto de resoluções da ANS demonstra um esforço no sentido de padronizar os procedimentos e informações necessários ao processo de regulação e assegurar o sigilo das informações de pacientes.

II.1.3) RESOLUÇÕES DO CONSELHO FEDERAL DE MEDICINA

O Conselho Federal de Medicina tem adotado diversas resoluções, que regulamentam, entre outras questões, o relacionamento médico-paciente, o relacionamento dos médicos com operadoras de planos de saúde, participação de pacientes em pesquisas, divulgação de estudos científicos e o prontuário médico do paciente. Estas resoluções complementam as legislações anteriores, principalmente em relação ao sigilo médico e avançam no reconhecimento e disciplina da utilização da tecnologia da informação na área de saúde, particularmente o prontuário eletrônico e a telemedicina.

O código de ética do Conselho Federal de Medicina (CFM, 1988) em diversos artigos, trata da questão do sigilo médico em relação aos dados de seus pacientes e à publicação de trabalhos científicos ou de outra natureza. Esses artigos estão transcritos abaixo, na íntegra:

Art. 11° - O médico deve manter sigilo quanto às informações confidenciais de que tiver conhecimento no desempenho de suas funções. O mesmo se aplica ao trabalho em empresas, exceto nos casos em que seu silêncio prejudique ou ponha em risco a saúde do trabalhador ou da comunidade.

É vedado ao médico:

Art. 70 - Negar ao paciente acesso a seu prontuário médico, ficha clínica ou similar, bem como deixar de dar explicações necessárias à sua compreensão, salvo quando ocasionar riscos para o paciente ou para terceiros.

Art. 102 - Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por justa causa, dever legal ou autorização expressa do paciente.

Parágrafo único: Permanece essa proibição: a) Mesmo que o fato seja de conhecimento público ou que o paciente tenha falecido. b) Quando do depoimento como testemunha. Nesta hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento.

Art. 103 - Revelar segredo profissional referente a paciente menor de idade, inclusive a seus pais ou responsáveis legais, desde que o menor tenha capacidade de avaliar seu problema e de conduzir-se por seus próprios meios para solucioná-lo, salvo quando a não revelação possa acarretar danos ao paciente.

Art. 104 - Fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos em programas de rádio, televisão ou cinema, e em artigos, entrevistas ou reportagens em jornais, revistas ou outras publicações leigas.

Art. 105 - Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.

Art. 106 - Prestar a empresas seguradoras qualquer informação sobre as circunstâncias da morte de paciente seu, além daquelas contidas no próprio atestado de óbito, salvo por expressa autorização do responsável legal ou sucessor.

Art. 108 - Facilitar manuseio e conhecimento dos prontuários, papeletas e demais folhas de observações médicas sujeitas ao segredo profissional, por pessoas não obrigadas ao mesmo compromisso.

Art. 109 - Deixar de guardar o segredo profissional na cobrança de honorários por meio judicial ou extrajudicial.

A resolução 1.605/2000 (CFM, 2000) continua a garantir a privacidade do paciente, impedindo que o médico revele dados e informações do prontuário ou ficha do paciente sem autorização do mesmo. Nos casos, onde a comunicação de doença é compulsória, o dever do médico restringe-se exclusivamente a comunicar tal fato à autoridade competente, sendo proibida a remessa do prontuário médico do paciente.

A resolução 1.642/2002 (CFM, 2002c) reforça a exigência do sigilo na relação entre os médicos e operadoras de planos de saúde, já que no seu artigo 1º, estabelece que *As empresas de seguro-saúde, de medicina de grupo, cooperativas de trabalho médico, empresas de autogestão ou outras que atuem sob a forma de prestação direta ou intermediação dos serviços médico-hospitalares devem respeitar o sigilo profissional, sendo vedado a essas empresas estabelecerem qualquer exigência que implique na revelação de diagnósticos e fatos de que o médico tenha conhecimento devido ao exercício profissional*.

A resolução 1643/2002 (CFM, 2002d) disciplina a prestação de serviços de telemedicina. No artigo 2º, esta resolução exige que *Os serviços prestados através da Telemedicina deverão ter a infra-estrutura tecnológica apropriada, pertinentes e obedecer as normas técnicas do CFM pertinentes à guarda, manuseio, transmissão de dados, confidencialidade, privacidade e garantia do sigilo profissional*.

A resolução 1638/2002 (CFM, 2002a) define o prontuário médico do paciente como instrumento sigiloso, legal e científico, torna obrigatória a criação da comissão de revisão de prontuários em instituições que prestam assistência médica, define os itens que devem compor o prontuário, e assegura a responsabilidade do preenchimento, guarda e manuseio dos prontuários, que cabem ao médico assistente, à chefia da equipe, à chefia da Clínica e à Direção técnica da unidade.

A resolução 1639/2002 (CFM, 2002b) reconhece a validade técnica e jurídica do prontuário eletrônico, ao aprovar as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", dispor sobre tempo de guarda dos prontuários, e estabelecer critérios para certificação dos sistemas de

informação. O artigo 7º desta resolução estabelece que "O Conselho Federal de Medicina e a Sociedade Brasileira de Informática em Saúde (SBIS), mediante convênio específico, expedirão, quando solicitados, a certificação dos sistemas para guarda e manuseio de prontuários eletrônicos que estejam de acordo com as normas técnicas especificadas no anexo a esta resolução". A SBIS (Sociedade Brasileira de Informática em Saúde) constituiu um grupo de trabalho para tratar desta questão e os trabalhos estão em andamento (SBIS, 2002).

O artigo123 do código de ética exige o consentimento informado do paciente para participação em pesquisas:
É vedado ao médico:
Art. 123 - Realizar pesquisa em ser humano, sem que este tenha dado consentimento por escrito, após devidamente esclarecido sobre a natureza e conseqüências da pesquisa.
Parágrafo único: Caso o paciente não tenha condições de dar seu livre consentimento, a pesquisa somente poderá ser realizada, em seu próprio benefício, após expressa autorização de seu responsável legal.

As normas para realização de pesquisas clínicas são mais detalhadas na resolução 1098 (CFM, resolução 1098), a qual adota o texto da declaração de Helsinqui para a realização desse tipo de pesquisa.

II.1.4) OUTROS TEXTOS

Em seu manual de padrões de acreditação hospitalar, o Consórcio Brasileiro de Acreditação (CBA, 2000) apresenta vários padrões a serem considerados durante o processo de acreditação hospitalar que se referem ao consentimento informado para participação em pesquisas, à garantia do sigilo, da segurança e da integridade dos dados e das informações e de sua transmissão para o ambiente externo. Esses padrões são apresentados abaixo (DE designa a função Direitos do Paciente e Familiares, Ética da Organização e Educação, GI designa a função Gerência da Informação):
DE 2.4 - O hospital informa ao paciente sobre como participar de pesquisas clínicas.

DE 2.4.1 - O paciente que escolhe participar de pesquisas clínicas é informado sobre os procedimentos adotados pelo hospital para protegê-lo.
DE 3 - O hospital adota políticas e procedimentos específicos para obter o consentimento informado do paciente.
DE 3.3 - O paciente expressa seu consentimento informado com relação a sua participação em pesquisa.
GI 2 - O hospital garante o sigilo, a segurança e a integridade dos dados e das informações.
GI 7.1.2 - O hospital garante a confidencialidade e a segurança dos dados sempre que utiliza ou envia dados a banco de dados externos.

O Ministério da Saúde tem emitido diversas portarias, disciplinando a transmissão de informações das unidades prestadoras de saúde para os órgãos públicos de gestão, seja para o caso de notificação compulsória de doenças, seja para fins de faturamento (SISAIH, SIASUS), seja padronizando informações, e constituindo bases de dados com estas informações. Nesse processo, dados provenientes do atendimento a pacientes, inclusive dados que permitem a identificação do mesmo são transmitidos por meio magnético aos órgãos de gestão. Já as bases secundárias disponíveis no DATASUS garantem o anonimato dos pacientes.

O ministério da saúde também tem se esforçado para construir as condições para a integração de seus sistemas de informação. Por exemplo, a medida provisória nº 3.947/GM, de 25 de novembro de 1998 (MS, 1997), estabelece atributos mínimos para a identificação do indivíduo assistido, do profissional, da instituição ou local de assistência, e do evento ou do atendimento realizado; estes atributos deveriam ser adotados, obrigatoriamente, por todos os sistemas e bases de dados do Ministério da Saúde, a partir de 1º de janeiro de 1999. Outra iniciativa importante é o Cartão Nacional de Saúde (MS, 1996). Um importante objetivo do projeto Cartão Nacional de Saúde é promover a integração entre os sistemas de informação utilizados no âmbito do Sistema Único de Saúde, sejam eles sistemas de base nacional ou sistemas de uso local. Para cada paciente, é atribuído um identificador único, o número do cartão nacional de saúde. Uma vez que o sistema permite o armazenamento das informações de atendimento vinculadas aos usuários e o acompanhamento da história clínica desse

mesmo usuário ao longo dos anos, é possível estabelecer associação e correlação entre diagnósticos, procedimentos, medicamentos prescritos, dentre outros, com impactos na elaboração de instrumentos de apoio à conduta dos profissionais de saúde. O sistema trabalha com padrões bem definidos, garantidos por tabelas corporativas residentes, o que permite a comparação entre as diversas informações coletadas. Por exemplo, para definir problemas de saúde é utilizada a CID 10 – Classificação Internacional de Doenças, para identificar os procedimentos executados ou solicitados são utilizadas as tabelas do Sistema de Informações Hospitalar e Ambulatorial (SIA-SUS e SIH-SUS), além de outras tabelas elaboradas especificamente para o Cartão Nacional de Saúde. Outra importante preocupação do projeto refere-se aos aspectos de ética e privacidade. Nesse sentido, merecem destaque os seguintes princípios considerados pelo sistema, incorporados na tecnologia desenvolvida e na política de acesso às informações proposta pelo Ministério da Saúde:

Os dados e informações registrados nos documentos e arquivos dos serviços de saúde, em qualquer meio, formato ou tecnologia, são propriedades da pessoa (paciente ou usuário) a quem se refere ou de quem descreve o estado de saúde e condição de vida.

2. Devem ser garantidos a essa pessoa a privacidade, o sigilo profissional e o segredo pessoal, em relação a seus dados e informações, por parte de todos os profissionais de saúde direta e indiretamente envolvidos na atenção integral a sua saúde.

3. São garantidas a confidencialidade, a integralidade e a segurança no registro, na transmissão, no armazenamento e na utilização dos dados e informações ind+ividuais existentes no serviço de saúde.

A implantação do Cartão Nacional de Saúde está prevista desde a Norma Operacional Básica do SUS de 1996. No entanto, a complexidade e o ineditismo do projeto fizeram com que somente em 1999 ele fosse iniciado. O processo de implantação em curso, considerado como projeto piloto, abrange 44 municípios brasileiros e atinge todas as regiões do País, alcançando cerca de 13 milhões de usuários dos SUS.

II.2) LEGISLAÇÃO INTERNACIONAL E DE OUTROS PAÍSES

O objetivo desta seção não é o de realizar uma revisão ampla da legislação internacional sobre o assunto em foco, mas apenas o de verificar as tendências que podem ser extraídas dessas legislações. O texto que se segue foi baseado no trabalho do Canadian Institutes of Health Research (CIHR, 2001), que realizou uma revisão de normas para a proteção de informações pessoais na pesquisa em saúde. A normas revisadas são normas e princípios emitidos por organismos internacionais (ONU, Conselho da Europa, Associação Médica Mundial, Organização para a Cooperação Econômica e Desenvolvimento, União Européia) e de alguns países: Austrália, Estados Unidos, França, Holanda, e Reino Unido.

Em parte, como resposta às atrocidades, excessos e abusos cometidos durante a 2ª guerra mundial, a comunidade internacional de adotou a privacidade como um princípio fundamental da moderna legislação internacional sobre os direitos humanos.

No julgamento por crimes contra a humanidade em Nuremberg, a corte emitiu o que ficou conhecido como código de Nuremberg. Este código delineia princípios relativos ao propósito da pesquisa, os riscos e benefícios ao indivíduo, os deveres e qualificações dos pesquisadores, mas o seu princípio fundamental é o que declara que o consentimento voluntário dos participantes humanos é absolutamente essencial. O código não incluiu conceitos como os de privacidade e confidencialidade.

Após o julgamento de Nuremberg, alguns organismos e países adotaram um conjunto de declarações formais e instrumentos legais que tiveram como objetivo promover e preservar a dignidade humana, exigindo o respeito à liberdade e autonomia humana, a privacidade e a confidencialidade.

Pelo menos três princípios da **Declaração Universal dos Direitos Humanos** (1948) delineiam elementos que seriam básicos para os princípios e leis de proteção dos dados que emergiram depois. O artigo 27 proclama que *todos tem o direito de participar livremente no …desenvolvimento científico e seus benefícios*. O artigo 12 identifica a privacidade como uma direito humano básico, declarando que *ninguém*

deve ser sujeito a interferências arbitrárias na sua privacidade, de sua família, residência ou correspondência, nem a ataques à sua honra e reputação. Todos têm o direito de proteção das leis contra tais interferências ou ataques. Para as situações de potencial conflito entre interesses da sociedade e do indivíduo, o artigo 29 proporciona um guia: *No exercício de seus direitos e liberdades, todos devem ser sujeitos somente a limitações que sejam determinadas por lei, somente com o propósito de garantir o devido reconhecimento e respeito pelos direitos de outros e para atender os requisitos justos de moralidade, ordem pública e bem-estar geral em uma sociedade democrática*.

Em 1950, o Conselho da Europa se apoiou na Declaração dos Direitos Humanos para definir a privacidade como um princípio fundamental na **Convenção para a Proteção dos Direitos Humanos e Liberdades Fundamentais: Convenção Européia sobre os Direitos Humanos**. Hoje, esta convenção está sendo aplicada em 40 países membros do Conselho da Europa. O artigo 8 estabelece que *Todos têm o direito ao respeito à sua vida privada e familiar….Não deverá haver nenhuma interferência de uma autoridade pública no exercício deste direito, exceto no que estiver de acordo com a lei e for necessário em uma sociedade democrática no interesse na segurança nacional, segurança pública ou estabilidade econômica do país, para a prevenção da desordem ou crime, para a proteção da saúde ou moral, ou para a proteção dos direitos e liberdades de outros*." Apesar de manter a substância da declaração dos direitos humanos, a Convenção Européia sobre os Direitos Humanos explicitam que a violação da privacidade pode ser efetuada naqueles itens previstos em lei e para a proteção da saúde ou moral. A necessidade de proteção à saúde seria adotada décadas depois na legislação e princípios internacionais de proteção de dados.

Em 1966, a Assembléia Geral da ONU adotou e abriu para assinatura o **Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP).** No mesmo ano, a ONU também adotou **o Pacto Internacional sobre os Direitos Econômicos, Sociais e Culturais (PIDESC)**. Estes pactos tiveram o objetivo de elaborar e proporcionar efeitos legais formais e a implementação dos princípios proclamados na Declaração

Universal. Os pactos foram assinados e ratificados por mais de 140 nações e começou a ser aplicado em 1976.

Pelo menos três artigos dos pactos dizem respeito à privacidade, consentimento, pesquisa e saúde. O artigo 17 do PIDCP segue os mesmos princípios do artigo 12 da Declaração Universal. Porém, o PDCP silencia em relação aos padrões que podem limitar o direito de privacidade. O PIDCP fornece um efeito legal explícito ao código de Nuremberg. Em seu artigo 7, ele declara que *ninguém deve ser submetido, sem o seu consentimento livre, a experiências médicas ou científicas*. Os artigos 12 e 15 do PIDESC respectivamente incluem , na enumeração dos direitos sociais, o direito de todos usufruírem os *benefícios do progresso científico e suas aplicações*. O artigo 15 destaca que as nações que assinam o PIDESC devem *respeitar a liberdade indispensável à pesquisa científica*.

A Associação Médica Mundial (AMM), fundada em 1947, tem emitido uma série de resoluções e declarações. Em 1948, a AMM adotou a **Declaração de Genebra**, que é um juramento do médico que foi posteriormente adotado no Código Internacional de Ética da AMM. Essa declaração lista diversas responsabilidades, incluindo o dever do *respeito aos segredos que são confiados a mim, mesmo após a morte do paciente*. Em 1964, a AMM adotou uma declaração detalhada de princípios éticos para a pesquisa médica que ficou conhecida como **Declaração de Helsinque**. Esta declaração sofreu revisões em 1975 e 2000. Nesta declaração, a privacidade e consentimento informado são considerados centrais para a preservação da integridade e dignidade de indivíduos humanos. Ao considerar os benefícios e ônus devido ao uso de computadores na medicina, a AMM, em 1973, adotou resoluções que reafirmaram a *importância vital da manutenção do segredo médico…para a proteção da privacidade de indivíduos como base para a relação de confiança entre o médico e o paciente*. Hoje, na sua versão revisada, a **Declaração sobre o Uso de Computadores na Medicina** busca harmonizar o dever de respeitar a confidencialidade, como proclamada na Declaração de Genebra, com a pesquisa médica que pode ser facilitada com o processamento eletrônico dos dados. A declaração estabelece que *não é uma quebra de confidencialidade liberar ou transferir informações confidenciais sobre a atenção à saúde necessárias para o propósito de se conduzir pesquisa*

científica…desde que as informações liberadas não identifiquem, diretamente ou indiretamente, qualquer paciente individual em qualquer relatório de tal publicação….

A partir de 1980, leis e princípios internacionais para a proteção de dados se seguiram, muitos dos quais se baseiam nos princípios gerais apresentados acima. Os países tendem então a refinar e aplicar essas leis a áreas particulares, tais como as envolvendo as informações de saúde de indivíduos. Entre este conjunto de leis, podem ser citadas:

- **Guias para a Proteção da Privacidade e o Fluxo Internacional de Dados Pessoais** (1980), da Organização para a Cooperação Econômica e Desenvolvimento;
- **Convenção para a Proteção de Indivíduos em relação ao Processamento Automático de Dados Pessoais** (1981), **Recomendação R97(5) sobre a Proteção de Dados Médicos** (1997), **Convenção para a Proteção dos Direitos Humanos e Dignidade do Ser Humano em relação à Aplicação da Biologia e Medicina** (1997), todas as três adotadas pelo Conselho da Europa;
- **Diretiva da União Européia 95/46/EC sobre a Proteção dos Indivíduos em relação ao Processamento de Dados Pessoais e o Livre Movimento de tais Dados** (1995), **Temas Éticos da Atenção à Saúde na Sociedade da Informação** (1999), **A Carta da União Européia dos Direitos Fundamentais** (2000), todas as três adotadas pela União Européia;
- **Guia para a Regulamentação dos Arquivos Computadorizados de Dados Pessoais** (1990), **Declaração sobre a Promoção dos Direitos do Paciente na Europa** (1994), **Declaração Universal sobre o Genoma Humano e Direitos Humanos** (1997), todas as três adotadas pela ONU.

Não é objetivo deste trabalho realizar uma análise comparada das resoluções acima. Elas levantam, entretanto, uma série de questões que devem ser abordadas por uma lei de proteção à privacidade. Estas questões são apresentadas, de maneira sucinta a seguir:

1. **Abrangência**: as resoluções variam em sua abrangência. Elas podem aplicar a dados públicos, a dados privados, ou a ambos; a dados processados e armazenados

automaticamente, a dados não automatizados, ou a ambos; a dados identificáveis ou não;

2. **Definições**: há variações sobre a definição do que sejam dados pessoais, identificação de indivíduos e dados médicos, processamento, e processamento automático;

3. **Proteções especiais, dados sensíveis**: as resoluções variam na especificação de dados que deveriam ser submetidos a proteção especial, padrões de proteção que deverão ser aplicados a sub-grupos específicos de dados, e na necessidade de consentimento para utilização dos dados sensíveis.

4. **Consentimento (padrões para a coleta, utilização e liberação de dados)**: as resoluções, em geral, exigem o uso do consentimento para o uso, processamento e liberação de dados personalizados, exceto em casos excepcionais previstos em lei. Os detalhes de como o consentimento é estabelecido e como o paciente deve ser informado variam de uma resolução para outra.

5. **Exceções e pesquisas**: exceções quanto ao dever da manutenção de sigilo podem ser apresentadas em caráter geral, ou serem mais detalhadas. Em alguns casos, padrões são estabelecidos para a utilização de dados em pesquisas e para a utilização de dados que identificam o indivíduo. O mesmo se aplica à utilização de dados secundários.

6. **Retenção de dados e segurança**: freqüentemente, as normas estabelecem padrões mínimos que devem ser respeitados para a garantia de segurança contra destruição, perda, acesso não autorizado, alteração ou liberação dos dados. A duração para a retenção dos dados, em geral, depende dos objetivos para os quais eles foram coletados, mas não devem ser retidos além do necessário.

Diversos países estabeleceram normas próprias, aplicando e aprofundando as resoluções discutidas acima dentro do contexto sócio, econômico, político e cultural de suas respectivas sociedades. Em geral, elas abrangem os itens listados acima e estabelecem regulamentos e restrições para a transferência de dados confidenciais para outros países.

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Chadwick et al (CHADWICK et al, 2000) desenvolveram um sistema de informação sobre diabetes que fornece uma conexão segura pela internet que permite a médicos, enfermeiras especializadas acesso ao sistema. A Tabela 1 apresenta um resumo dos problemas de segurança e a solução para o acesso ao sistema via internet.

Tabela 1 – Resumo de problemas de segurança e suas soluções para o sistema de informação sobre diabetes (CHADWICK et al, 2000)

Problema	Descrição	Solução
Autenticação do usuário	Como o sistema sabe que uma identidade remota de usuário é genuína?	Autenticação forte do usuário
Estabelecimento de direitos de acesso	Que porções do banco de dados um usuário tem acesso?	Controle de acesso ao banco de dados
Captura não autorizada dos dados	Como garantimos que ninguém possa obter uma cópia dos dados que estão sendo transferidos pela internet do sistema para um usuário remoto ?	Criptografia das mensagens
Entrada na rede da instituição	Como protegemos a intranet da entrada de tráfico indesejado, ao mesmo tempo que permitimos a passagem de tráfico desejado ?	Firewall entre a intranet e a internet
Interface fácil de usar	Como desenvolvermos uma interface simples, mas fácil de usar que a maioria dos usuários estará familiarizado e necessitará de treinamento mínimo para usar e que seja de baixo custo ?	Navegadores da web
Fonte de dados correta	Como os usuários remotos sabem que eles acessaram o sistema correto e não um sítio mascarado como se fosse o	Autenticação forte do sistema

sistema ?

Os objetivos de segurança das informações na atenção à saúde são (BARROWS e CLAYTON, 1996):

1. Garantir a privacidade de pacientes e a confidencialidade dos dados de cuidados em saúde (evitar a revelação não autorizada de informações);
2. Garantir a integridade dos dados (evitar a modificação não autorizada de informações);
3. Garantir a disponibilidade dos dados para pessoas autorizadas (evitar a indisponibilidade não intencional ou não autorizada de informações ou recursos).
4. Não repúdio (capacidade de um sistema de provar que um usuário executou determinada ação no sistema).

Em conformidade com os objetivos delineados acima, a Tabela 1 apresenta uma parte dos aspectos de segurança que estão presentes na utilização de sistemas de informação. Outros aspectos dizem respeito à segurança física das instalações, proteção contra destruição, educação dos usuários, penalidades, etc. O *Columbia-Presbyterian Medical Center* levantou 14 itens que devem compor uma política de segurança para sistemas de informação (BARROWS e CLAYTON, 1996):

1. Autenticação do usuário;
2. Segurança física do centro de processamento de dados, cópias de segurança e recuperação de desastres;
3. Controle de acesso aos recursos do sistema;
4. Propriedade dos dados, deveres e responsabilidades dos proprietários dos dados;
5. Políticas de proteção dos dados - proteções consistentes e aceitáveis a serem proporcionadas por sistemas que cruzem fronteiras organizacionais e funcionais, antecipação de barreiras à sua implementação e medidas de punição, em caso de abuso de privilégios de acesso ao sistema;
6. Implementação de segurança nos sistemas;
7. Segurança de cópias impressas de documentos eletrônicos;
8. Integridade do sistema;
9. Perfis de usuários - definição de tipos de usuários e papéis que servem para distinguir as necessidades funcionais e níveis de segurança;

10.Temas legais - relacionados ao uso e mau uso do sistema e que podem resultar em processos ou preocupações legais para a organização;
11.Identificação e resolução de problemas - auditoria, detecção e notificação de invasões, mecanismo de detecção e notificação para outros tipos de problemas de segurança;
12.Segurança da rede de dados;
13.Consentimento informado por parte dos pacientes para o uso de dados relativos aos mesmos;
14.Educação dos usuários.

Existem boas orientações para se estabelecer uma política de segurança em ambientes de informática e desenvolvimento de software (ALBUQUERQUE e RIBEIRO, 2002; CARUSO e STEFFEN, 1999). Muitas dessas orientações se baseiam em normas internacionais (Normas ISO – International Organization for Standardization) e nacionais (ABNT – Associação Brasileira de Normas Técnicas).

O estado da arte da tecnologia de computadores, telecomunicações e de software permite a construção de sistemas de informação que minimizem o risco de quebra de segurança e se elas ocorrerem, ser possível de serem detectadas e verificar os responsáveis pela quebra. Entretanto, a questão da privacidade e confidencialidade de dados não é uma questão puramente técnica, pois exige o estabelecimento de uma política que defina que dados devem ser protegidos, em que nível, quem poderá ter acesso aos mesmos, quais as operações que cada usuário pode realizar sobre os dados, para onde eles podem ser transferidos, por quanto tempo eles estarão disponíveis e quem determina quem pode ter acesso aos dados. Em referência ao prontuário eletrônico, princípios freqüentemente citados para a sua implementação são: o consentimento do paciente para o acesso ao prontuário, liberdade de o paciente verificar a lista dos acessos ao seu prontuário e que operações foram efetuadas, permissão para o paciente realizar correções em seus prontuários e a exigência do consentimento do paciente para que seus dados sejam utilizados com propósitos outros que não a atenção direta à sua saúde (BARROWS e CLAYTON, 1996; RIND et al, 1997; DICK et al, 1997; DENLEY E SMITH, 1999; MANDL et al, 2001). Princípios semelhantes, respeitando as devidas características particulares, podem ser

aplicados a dados e informações de instituições como, por exemplo, as operadoras de planos e prestadores de assistência à saúde.

A legislação nacional incorporou diversos elementos de uma política de segurança de sistemas de informação. O capítulo V do Decreto 4.553 (BRASIL, 2002b), apresenta, entre outras, as seguintes normas:

Art. 42. Ressalvado o disposto no parágrafo único do art. 44, os programas, aplicativos, sistemas e equipamentos de criptografia para uso oficial no âmbito da União são considerados sigilosos e deverão, antecipadamente, ser submetidos à certificação de conformidade da Secretaria Executiva do Conselho de Defesa Nacional.

Art. 43. Entende-se como oficial o uso de código, cifra ou sistema de criptografia no âmbito de órgãos e entidades públicos e instituições de caráter público.

Parágrafo único. É vedada a utilização para outro fim que não seja em razão do serviço.

Art. 44. Aplicam-se aos programas, aplicativos, sistemas e equipamentos de criptografia todas as medidas de segurança previstas neste Decreto para os documentos sigilosos controlados e os seguintes procedimentos:

I - realização de vistorias periódicas, com a finalidade de assegurar uma perfeita execução das operações criptográficas;

II - manutenção de inventários completos e atualizados do material de criptografia existente;

III - designação de sistemas criptográficos adequados a cada destinatário;

IV - comunicação, ao superior hierárquico ou à autoridade competente, de qualquer anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de dados ou informações criptografados; e

V - identificação de indícios de violação ou interceptação ou de irregularidades na transmissão ou recebimento de dados e informações criptografados.

Parágrafo único. Os dados e informações sigilosos, constantes de documento produzido em meio eletrônico, serão assinados e criptografados mediante o uso de certificados digitais emitidos pela Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).

Art. 46. A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica,

deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento.
Art. 47. Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo secreto, confidencial e reservado só poderão integrar redes de computadores que possuam sistemas de criptografia e segurança adequados a proteção dos documentos.
Art. 48. O armazenamento de documentos sigilosos, sempre que possível, deve ser feito em mídias removíveis que podem ser guardadas com maior facilidade.

As normas técnicas para o uso de sistemas informatizados para a guarda e manuseio do prontuário médico, constantes na Resolução 1639/2002 do Conselho Federal de Medicina (CFM, 2002b), são mais detalhadas nos requisitos de segurança de sistemas de informação. Esses requisitos são apresentados abaixo:
Integridade da Informação e Qualidade do Serviço *– O sistema de informações deverá manter a integridade da informação através do controle de vulnerabilidades, de métodos fortes de autenticação, do controle de acesso e métodos de processamento dos sistemas operacionais conforme a norma ISO/IEC 15408, para segurança dos processos de sistema.*
Cópia de Segurança *– Deverá ser feita cópia de segurança dos dados do prontuário pelo menos a cada 24 horas. Recomenda-se que o sistema de informação utilizado possua a funcionalidade de forçar a realização do processo de cópia de segurança diariamente. O procedimento de back-up deve seguir as recomendações da norma ISO/IEC 17799, através da adoção dos seguintes controles:*
Documentação do processo de backup/restore;
As cópias devem ser mantidas em local distante o suficiente para livrá-las de danos que possam ocorrer nas instalações principais;
Mínimo de três cópias para aplicações críticas;
Proteções físicas adequadas de modo a impedir acesso não autorizado;
Possibilitar a realização de testes periódicos de restauração.
Bancos de Dados *– Os dados do prontuário deverão ser armazenados em sistema que assegure, pelo menos, as seguintes características:*
Compartilhamento dos dados;
Independência entre dados e programas;

Mecanismos para garantir a integridade, controle de conformidade e validação dos dados;

Controle da estrutura física e lógica;

Linguagem para a definição e manipulação de dados (SQL – Standard Query Language);

Funções de auditoria e recuperação dos dados.

***Privacidade e Confidencialidade** – Com o objetivo de garantir a privacidade, confidencialidade dos dados do paciente e o sigilo profissional, faz-se necessário que o sistema de informações possua mecanismos de acesso restrito e limitado a cada perfil de usuário, de acordo com a sua função no processo assistencial:*

Recomenda-se que o profissional entre pessoalmente com os dados assistenciais do prontuário no sistema de informação;

A delegação da tarefa de digitação dos dados assistenciais coletados a um profissional administrativo não exime o médico, fornecedor das informações, da sua responsabilidade desde que o profissional administrativo esteja inserindo estes dados por intermédio de sua senha de acesso;

A senha de acesso será delegada e controlada pela senha do médico a quem o profissional administrativo está subordinado;

Deve constar da trilha de auditoria quem entrou com a informação;

Todos os funcionários de áreas administrativas e técnicas que, de alguma forma, tiverem acesso aos dados do prontuário deverão assinar um termo de confidencialidade e não-divulgação, em conformidade com a norma ISO/IEC 17799.

***Autenticação** – O sistema de informação deverá ser capaz de identificar cada usuário através de algum método de autenticação. Em se tratando de sistemas de uso local, no qual não haverá transmissão da informação para outra instituição, é obrigatória a utilização de senhas. As senhas deverão ser de no mínimo 5 caracteres, compostos por letras e números. Trocas periódicas das senhas deverão ser exigidas pelo sistema no período máximo de 60 (sessenta) dias. Em hipótese alguma o profissional poderá fornecer a sua senha a outro usuário, conforme preconiza a norma ISO/IEC 17799. O sistema de informações deve possibilitar a criação de perfis de usuários que permita o controle de processos do sistema.*

***Auditoria** – O sistema de informações deverá possuir registro (log) de eventos, conforme prevê a norma ISO/IEC 17799. Estes registros devem conter:*

A identificação dos usuários do sistema;
Datas e horários de entrada (log-on) e saída (log-off) no sistema;
Identidade do terminal e, quando possível, a sua localização;
Registro das tentativas de acesso ao sistema, aceitas e rejeitadas;
Registro das tentativas de acesso a outros recursos e dados, aceitas e rejeitadas.
Registro das exceções e de outros eventos de segurança relevantes devem ser mantidos por um período de tempo não inferior a 10 (dez) anos, para auxiliar em investigações futuras e na monitoração do controle de acesso.
***Transmissão de Dados** – Para a transmissão remota de dados identificados do prontuário, os sistemas deverão possuir um certificado digital de aplicação única emitido por uma AC (Autoridade Certificadora) credenciada pelo ITI responsável pela AC Raiz da estrutura do ICP-Brasil, a fim de garantir a identidade do sistema.*
***Certificação do software** – A verificação do atendimento destas normas poderá ser feita através de processo de certificação do software junto ao CFM, conforme especificado a seguir.*
***Digitalização de prontuários** - Os arquivos digitais oriundos da digitalização do prontuário médico deverão ser controlados por módulo do sistema especializado que possua as seguintes características.*
Mecanismo próprio de captura de imagem em preto e branco e colorida independente do equipamento scanner;
Base de dados própria para o armazenamento dos arquivos digitalizados;
Método de indexação que permita criar um arquivamento organizado, possibilitando a pesquisa futura de maneira simples e eficiente;
Mecanismo de pesquisa utilizando informações sobre os documentos, incluindo os campos de indexação e o texto contido nos documentos digitalizados, para encontrar imagens armazenadas na base de dados;
Mecanismos de controle de acesso que garantam o acesso a documentos digitalizados somente por pessoas autorizadas.

Um grupo de trabalho da Sociedade Brasileira de Informática em Saúde (SBIS, 2003) foi criado para definir a metodologia de certificação e detalhar os requisitos que serão analisados nos sistemas informatizados de gerenciamento do prontuário médico. Diversos subgrupos estão analisando aspectos específicos do processo:

- Subgrupo 1: Processo de certificação, com a missão de detalhar o processo de certificação a ser implantado pela SBIS;
- Subgrupo 2: Segurança, com a missão de detalhar os requisitos de segurança para fins de certificação;
- Subgrupo 3: Conteúdo e Funcionalidades, com a missão de detalhar os requisitos de conteúdo e funcionalidades que deverão estar presentes nos sistemas informatizados de prontuário eletrônico.

Essa iniciativa deve servir de inspiração para estender este processo de certificação aos sistemas de informação em saúde em geral.

DISCUSSÃO

Este estudo não se propôs a uma análise exaustiva de toda a legislação brasileira e internacional sobre o assunto em foco. Por exemplo, apesar de diversas resoluções do Conselho Federal de Medicina terem sido consultadas, o mesmo não ocorreu com os respectivos órgãos de outras associações profissionais. Entretanto, acreditamos que o material apresentado fornece subsídios básicos para uma reflexão inicial e nos permite formular algumas recomendações para o encaminhamento posterior da questão.

O material analisado neste trabalho mostra que a legislação sobre o sigilo de dados e informações na área de saúde está dispersa em diversas resoluções, leis, decretos, códigos, constituição, etc, adotadas por diversos órgãos. Conseqüentemente, o âmbito de aplicação das normas é variado: algumas se aplicam à administração pública, outras a associações profissionais, outras à assistência suplementar à saúde, outras à sociedade como um todo, etc. A legislação apresenta uma série de avanços na normatização, no Brasil, do tema em foco. Assim diversos itens já são objeto de normatização: direito de acesso e correção de informações em bancos de dados, sigilo profissional, segurança de sistemas de informações, consentimento informado dos pacientes para a realização de pesquisas e para a divulgação de seus dados, dentre outros. É necessário, porém, consolidar todas essas conquistas em uma legislação única e abrangente que se aplique ao Sistema de Saúde como um todo, a partir da qual todos os atores no sistema se pautem. Por outro lado, alguns itens precisam ser aprofundados conforme a discussão que se segue.

Em primeiro lugar, consideremos o sigilo de dados e informações de pacientes. Este sigilo é fundamental para garantir a confiança na relação médico-paciente, pois é em função do mesmo que o paciente revela detalhes de sua vida pessoal que podem ser essenciais para a definição da melhor conduta para a solução de seus problemas de saúde. Não é por outra razão que este princípio é consagrado em diversos princípios e normas nacionais e internacionais. Por outro lado, nos sistemas modernos de atenção à saúde, outras categorias profissionais também participam da atenção aos pacientes: enfermeiros, psicólogos, psiquiatras, nutricionistas, fisioterapeutas, e assistentes

sociais. As resoluções das respectivas associações profissionais não foram aqui analisadas, mas o princípio do sigilo profissional deve ser aplicado também para estas categorias.

Conforme ressaltado na introdução deste trabalho, outras questões de natureza financeira, administrativa, gerencial, e científica demandam a coleta e análise de dados e informações obtidas a partir dos prontuários dos pacientes ou coletadas diretamente para um objetivo específico. Por exemplo, nas instituições prestadoras de atenção à saúde, os funcionários da seção de faturamento freqüentemente têm que ter acesso ao prontuário dos pacientes para extrair informações para a fatura, especialmente nas cobranças de AIH, que possuem um grande número de regras. A legislação deve prever outros usos para o conteúdo registrado do contato direto do paciente com o sistema de saúde, disciplinar este uso e restringir os dados que podem ser acessados somente àqueles estritamente necessários ao objetivo em questão. Sempre que possível, os dados utilizados **não devem identificar o paciente**, exceto naquelas exceções devidamente justificadas, que precisam ser explicitadas.

Diversas fontes recomendam a necessidade do consentimento informado para a utilização dos dados de pacientes para fins de pesquisa de intervenções clínicas, pesquisas na área de saúde pública, e avaliação de serviços, incluindo a utilização de dados secundários. Este consentimento pode ser implícito, quando o indivíduo está ciente de que seus dados estarão disponíveis para outra finalidade, além da atenção à saúde, e que ele(a) tem o direito de recusar, porém ele não faz nenhuma objeção. Embora o consentimento explícito e por escrito seja essencial para a maior parte dos estudos de qualquer intervenção, ele é um requisito não realista em estudos observacionais e auditorias, principalmente se eles se baseiam em uma quantidade muito grande de dados retrospectivos. Viéses sistemáticos poderiam invalidar os resultados de estudos observacionais se as pessoas fossem excluídas porque elas não consentiram com a utilização dos dados. Por exemplo, a obtenção de consentimento poderia ser viciado pela idade ou sexo, e pelo fato de indivíduos estarem mortos, não serem encontrados, estarem impedidos cognitivamente, etc. Informação anônima não é freqüentemente suficiente, porque dados que identificam o paciente podem ser necessários para evitar duplicação de dados e permitir o seguimento longitudinal dos

pacientes (AL-SHAHI e WARLOW, 2000; VERITY e NICOL, 2002). Assim, exceções talvez devam ser previstas em relação à necessidade do consentimento informado, embora existam evidências de que os pacientes tendem a fornecer o consentimento quando são adequadamente informados sobre o objetivo dos estudos (MANNING, 2002; WILLISON, 2003). Deve-se prever que a legislação para a proteção de dados, em suas normas relativas ao consentimento informado para a realização de pesquisas em saúde pública, pode gerar incertezas e inconsistências na sua aplicação, dificultando a realização de estudos, particularmente os multicentros; isto acontece especialmente no início da aplicação de uma lei (STROBL et al, 2000). A legislação deve regulamentar a utilização de bases de dados secundárias para a pesquisa em saúde, em particular quando estas bases identificam univocamente o paciente.

Outra questão freqüentemente abordada é o direito de o paciente ser informado sobre o conteúdo dos bancos de dados sobre ele(a) e solicitar correções quando julgar necessárias e do direito de o mesmo determinar o que pode ser acessado e por quem. Parece ser um princípio razoável de que todas as instituições ou profissionais que detenham dados de terceiros informem aos mesmos a existência desses arquivos. Por outro lado, o acesso irrestrito de pacientes a bancos de dados, particularmente os do prontuário, deve ser visto com reservas. A legislação deve prever exceções a esta regra, sempre que o acesso possa resultar em prejuízo à saúde do paciente, ou a critério do profissional de saúde, quando o mesmo julgar que o acesso não deve ser liberado. O prontuário eletrônico e os sistemas de informação, em geral, podem oferecer facilidades para a implementação dessas regras: registro de todas as transações no banco de dados, quem realizou as alterações, registro das razões de por que o acesso não é liberado, etc. Em condições normais, o direito de o paciente determinar quem pode acessar o que em seu prontuário é um princípio que deve ser considerado, respeitando as exceções que eventualmente possam ocorrer, conforme assinalado acima. Isto se aplica a prontuários, como também a outros arquivos de dados. Um exemplo concreto é o caso de sistemas de laboratórios que divulgam os resultados de pacientes pela internet. Normas específicas para estes sistemas devem existir no que refere ao controle de acesso aos exames, segurança dos sistemas e direitos do paciente de controlar a liberação dos exames. O mesmo se aplica também a outros sistemas de informação que lidam com dados de pacientes.

A relação paciente-profissional de saúde é uma relação singular. A natureza deste relacionamento é diferente das outras relações existentes no sistema de saúde. A privacidade dos dados e informações de pacientes é protegida devida à natureza íntima das informações clínicas e da necessidade de se preservar o relacionamento terapêutico entre o prestador e o recipiente da atenção. O paciente não possui escolha ao revelar informações pessoais para garantir um processo eficaz de diagnóstico e tratamento, e as regras de confidencialidade visam a resguardar o relacionamento que aí se desenvolve (GOSTIN, 1997). O mesmo não se aplica aos dados de prestadores da atenção à saúde, operadoras de planos de saúde, agências reguladoras, e outras entidades do Sistema de Saúde. Todas essas entidades resultam de um processo sócio, econômico, político e cultural cujo objetivo central é o de oferecer à população o acesso à saúde. As informações e dados dessas entidades, que permitem a avaliação de desempenho, auditorias, o planejamento e formulação de políticas de saúde não são da mesma natureza daquelas derivadas da relação paciente-profissional de saúde. As normas de privacidade e confidencialidade que aí se aplicam devem ter como objetivo evitar o uso indevido de informações e preservar a ética e a concorrência leal no relacionamento entre as entidades...

É claro que, para cumprir seus objetivos, os prestadores de assistência à saúde necessitam de informações dos pacientes, de seus profissionais e dos atendimentos realizados em suas unidades; as operadoras necessitam de cadastros de beneficiários, dos prestadores a elas credenciados e dos atendimentos por elas ressarcidos; as agências reguladoras precisam obter informações das operadoras de naturezas diversas; e os consumidores devem dispor de informações das operadoras de planos de saúde e prestadoras de assistência à saúde. Necessidades de dados e informações ocorrem em outras instâncias como órgãos governamentais, instituições de ensino e pesquisa, etc. A legislação que se aplica nesses casos deve considerar os seguintes pontos:

1. restringir a coleta e a transferência de dados entre entidades ao mínimo necessário para cumprir os objetivos previstos. Sempre que possível, o conteúdo de dados deve ser especificado para cada finalidade. Esses dados devem ser agrupados em níveis

diferentes de sigilo, os dados identificadores devem ser separados dos outros conjuntos de dados e uma política de controle de acesso deve ser estabelecida para cada nível;

2. o uso dos dados deve se restringir aos objetivos para os quais eles foram coletados, o fluxo de dados entre entidades deve obedecer a normas de segurança unificadas;

3. as instituições devem estabelecer políticas explícitas para o cumprimento dessas normas e punições severas para quem viole as normas estabelecidas. A resolução RN 21 da ANS é um avanço neste sentido; mas ela tem que ser aprofundada e estendida para outras situações;

4. as entidades do Sistema de Saúde devem ter o direito de evitar a liberação indevida de suas informações e de acompanhar a coleta, o uso e disseminação de dados e informações que possam afetar a sua reputação;

5. a legislação deve ser desenvolvida paulatinamente, à medida que as propostas sejam formuladas e acordadas.

A sociedade está presenciando a disseminação do desenvolvimento e utilização de sistemas de informações para a coleta, análise e divulgação de informações na área de saúde. O volume de dados e a complexidade do sistema de saúde não dá mais lugar ao processamento manual de dados. Temores são despertados em relação aos riscos da possibilidade do acesso e uso indevido a dados de pacientes e instituições proporcionados por tais sistemas. Entretanto, deve ser enfatizado que os sistemas tradicionais de arquivos não são isentos de riscos de violação de sigilo. O prontuário em papel, por exemplo não permite se obter uma auditoria acurada de quem teve acesso a ele ou que porções do mesmo foram manuseadas, são facilmente alterados pela remoção ou substituição de documentos e não permite que se restrinja a certas classes de usuários o acesso somente a grupos específicos de dados e informações. Os controles acima descritos são mais fáceis de serem implementados no prontuário eletrônico.

A moderna tecnologia da informação permite o desenvolvimento de sistemas de informações que minimizem o risco de quebra de sigilo: *firewalls*, controle de acesso definido em função da necessidade de conhecer, registro dos acessos (quem fez o que

a quem), proteção física dos ambientes, proteção dos dados contra a destruição e perdas, cópias de segurança, e outros. Apesar de freqüentes notícias sobre quebras de segurança em sistemas de informação provocada por *crackers*, *hackers*, vírus, etc, deve ser lembrado que não existe segurança perfeita em nenhum tipo de sistema (eletrônico ou não), que diferentes sistemas apresentam diferentes níveis de segurança e que as exigências de segurança devem ser analisadas juntamente com os custos, riscos e necessidade de uso das informações. A ameaça mais comum à confidencialidade é **o acesso inapropriado às informações por usuários autorizados**. Tal risco é tão grande ou maior quando os dados estão armazenados em papel (Shortliffe, 1998; Rind et al, 1997). Um meio de reduzir esta ameaça é o de estabelecer punições severas para usuários que violem os direitos de indivíduos ou instituições. Assim, uma legislação adequada, que defina políticas e sanções, é tão importante para a proteção de informações quanto às técnicas para a criação de *firewalls* e garantir a identificação e autenticação de usuários.

O Decreto 4.553 (BRASIL, 2002b), a resolução 1639 do Conselho Federal de Medicina (CFM, 2002b), e o grupo de trabalho da SBIS para a certificação de softwares (SBIS, 2002) representam avanços importantes na área de segurança de sistemas de informação. Este tipo de trabalho deve ser estimulado e estendido a outros sistemas de informação na área de saúde.

A Agência Nacional de Saúde Suplementar, em diversas resoluções, busca padronizar os formulários para a coleta de informações. O uso de sistemas informatizados que padronizam e integram as informações é a melhor solução para garantir a segurança dos dados, sem impedir o acesso aos usuários autorizados. Planilhas eletrônicas e formulários em papel estão mais propensos a acessos não autorizados. A legislação deve incentivar o desenvolvimento e implantação de sistemas de informação, respeitando os requisitos de segurança e controle de acesso, conforme previsto em parágrafo anterior.

V) RECOMENDAÇÕES

A legislação brasileira tem refletido, especialmente nos último anos, uma preocupação com a questão do sigilo das informações, que se reflete na adoção de diversas resoluções e decretos e na criação de um grupo de trabalho para tratar da questão da certificação de software de prontuário eletrônico. Este trabalho deve ser complementado pelo estabelecimento de uma legislação que consolide as diversas normas publicadas em uma legislação específica para a área da saúde e que leve em conta outros aspectos até então não contemplados ou não claramente definidos. Assim sendo, este trabalho oferece as recomendações a seguir para o encaminhamento desta questão. Algumas propostas apresentadas são baseadas em artigo de Gostin (GOSTIN, 1997):

1. Criação de uma comissão de segurança e proteção dos dados. Esta comissão faria uma revisão abrangente da legislação nacional e internacional e proporia padrões de segurança e privacidade; monitorizaria e avaliaria a implementação de padrões estabelecidos por estatutos, regulamentos, e protocolos, solicitaria ou conduziria pesquisas, estudos, e investigações, e trabalharia para estimular o desenvolvimento de práticas de privacidade e segurança que responderiam aos objetivos de prover a atenção à saúde e a segurança e a confidencialidade dos dados. A composição deste comitê deveria refletir os diversos componentes do Sistema de Saúde e as diversas competências necessárias para o cumprimento de sua missão;
2. A legislação federal deve estabelecer uma proteção à privacidade da informação em saúde que seja uniforme e abrangente. Ela deve englobar todos as informações em saúde, não importando o meio (papel, microfilme, ou eletrônico), a localização (arquivos, armazéns, trânsito) ou usuário ou custodiante (governo, provedor, ou organização privada). Penalidades efetivas por quebras de privacidade devem ser estabelecidas. Uma estrutura nacional deve ser baseada no seguinte código: indivíduos devem ter o direito de controlar o uso de dados pessoais, sistemas secretos de dados não devem ser permitidos, indivíduos devem ter o direito de revisar e corrigir os dados pessoais, e os dados seriam coletados e usados somente para importantes propósitos da atenção à saúde. Os pacientes devem ser informados sobre a existência de documentos ou bancos de dados com informações a seu respeito;
3. Os pacientes devem poder consentir sobre a coleta e uso de informações pessoais. Os pacientes têm o direito de saber e consentir na coleta e uso de informações

identificadoras, o tempo que esta informação pode ser armazenada e as circunstâncias sob as quais ela pode ser apagada, e o grau em que terceiros possam obter acesso. A aquisição, armazenamento, uso, e transmissão de dados devem ser realizados com o consentimento dos pacientes. As exceções a este princípio devem se restringir ao mínimo necessário e serem devidamente justificadas. Consideração especial deve ser dada à área de pesquisa (clínica e de saúde pública), e ao uso de bases de dados secundários;

4. As entidades do Sistema de Saúde (prestadores de atenção, operadoras de planos de saúde, agências reguladoras, órgãos públicos, etc) devem aderir ao princípio da revelação menos intrusiva. A liberação de informações pelos prestadores de saúde deve se restringir aos dados que são menos prováveis de identificar o paciente e revelar fatos pessoais sensíveis e ao menor número de pessoas necessárias para atingir o propósito declarado para a liberação. Princípio semelhante deve regular o uso e a liberação de informações das entidades que compõem o sistema de saúde;

5. As entidades do Sistema de Saúde devem ter o direito de evitar a liberação indevida de suas informações e de acompanhar a coleta, o uso e disseminação de dados e informações que possam afetar a sua reputação;

6. O uso de sistemas de informação deve ser estimulado. Uma infra-estrutura de segurança para sistemas de informação, abrangendo toda a sociedade deve ser estabelecida, incluindo: autenticação de usuários, controle de acesso, trilhas de auditoria, recuperação de desastres, proteção de pontos remotos de acesso, criptografia de todos os dados identificadores antes da transmissão em redes públicas, etc. O conteúdo de dados deve ser especificado para cada finalidade de uso. Os dados devem ser agrupados em níveis diferentes de sigilo, os dados identificadores devem ser separados dos outros conjuntos de dados e uma política de controle de acesso deve ser estabelecida para cada nível. Requisitos mínimos de segurança para os sistemas de informação que lidam com dados sigilosos devem ser especificados e os softwares que lidam com esses dados devem respeitar os requisitos estabelecidos.

REFERÊNCIAS

ANS - AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. Resolução RDC Nº 3, de 20 de JANEIRO de 2000a. Aprova normas de fornecimento de informações para cadastros de

beneficiários. Disponível em:

http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC Nº 4, de 18 de fevereiro de 2000b. Dispõe sobre alteração de rotina do registro provisório de produtos, e dá outras providências. Disponível em:

http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC Nº 5, de 18 de fevereiro de 2000c. Aprova normas sobre os procedimentos administrativos para requerimento e concessão de registro provisório das operadoras de Planos Privados de Assistência à Saúde. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC Nº 22, de 30 de MAIO de 2000d. Cria instrumento para acompanhamento econômico-financeiro das Operadoras. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC Nº 23, de 6 de JUNHO de 2000e. Altera a Resolução RDC nº 10, de 3 de março de 2000, institui Ficha de Compensação, estabelece padronização para o envio de informações que menciona e dá outras providências. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC Nº 24, de 13 de JUNHO de 2000f. Dispõe sobre a aplicação de penalidades às operadoras de planos privados de assistência à saúde. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC Nº 29, de 26 de JUNHO de 2000g. Estabelece normas para reajuste das contraprestações pecuniárias dos planos e produtos privados de assistência suplementar à saúde. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC n^0 64, de 10 de abril de 2001a. Dispõe sobre a designação de médico responsável pelo fluxo de informações relativas à assistência médica prestada aos consumidores de planos privados de assistência à saúde. Disponível em:

http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC nº 66, de 03 de maio de 2001b. Estabelece normas para reajuste das contraprestações pecuniárias dos planos privados de assistência suplementar à saúde . Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução RDC N.º 85, de 21 de setembro de 2001c. Institui o Sistema de Informações de Produtos – SIP para acompanhamento da assistência prestada aos beneficiários de planos privados de assistência à saúde. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

_____ . Resolução Normativa RN n^o 21, de 12 de dezembro de 2002. Dispõe sobre a proteção das informações relativas à condição de saúde dos consumidores de planos privados de assistência à saúde e altera a Resolução RDC n^0 24, de 13 de junho de 2000. Disponível em: http://www.ans.gov.br/portal/site/legislacao/y_legislacao_regulamentacoes_interna_751.asp?regulamentacao_titulo=Normativas. Acesso em: 24 jun. 2003.

ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no Desenvolvimento de Software**. Rio de Janeiro: Editora, 2002.

AL-SHAHI, R.; WARLOW, C. Using patient-identifiable data for observational research and audit. Overprotection could damage the public interest. **British Medical Journal**, v. 321, p. 1031-1032, 2000.

BARROWS JR., R.C.; CLAYTON, P.D. Privacy, Confidentiality, and Electronic Medical Records. **Journal of the American Medical Informatics Association**, v. 3, n. 2, p. 139-148, 1996.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/DEL2848.htm . Acesso em: 21 jul. 2003.

_____ . **Lei nº 5.869, de 11 de janeiro de 1973**. Institui o código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L5869.htm . Acesso em: 21 jul. 2003.

_____ . **Constituição da República Federativa do Brasil**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/nova-constituicao/main.htm. Acesso em: 15 jul 2003.

_____ .. **Lei Nº 8078, de 11 de setembro de 1990**. Dispõe sobre a proteção ao consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm . Acesso em: 21 jul. 2003.

_____ . **Lei nº 9.961, de 28 de janeiro de 2000**. Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências. Disponível em: http://www.ans.gov.br/portal/site/legislacao/legislacao_lei_criacao.asp. Acesso em: 24 jun. 2003.

_____ . **Medida Provisória nº 2.200-2, de 24 de Agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/MPV/2200-2.htm. Acesso em: 16 jul. 2003

_____ . **Lei n^0 10.406, de 10 de janeiro de 2002a**. Institui o código civil. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm . Acesso em: 21 jul. 2003.

_____ . **Decreto n^0 4.553, de 27 de dezembro de 2002b**. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm . Acesso em: 02 jul. 2003.

CARUSO, C.A.A.; STEFFEN, F.D. **Segurança em Informática e de Informações**. 2ª edição, São Paulo: Editora SENAC, 1999.

CBA - CONSÓRCIO BRASILEIRO DE ACREDITAÇÃO DE SISTEMAS E SERVIÇOS DE SAÚDE. Manual de Padrões de Acreditação Hospitalar. Primeira edição, Rio de Janeiro: UERJ, 2000, 236p.

CHADWICK, D.W.; CROOK, P.J.; YOUNG, A.J.; MCDOWELL, D.M.; DORNAN, T.L.; NEW, J.P. Using the Internet to Access Confidential Patient Records: a Case Study. **British Medical Journal**, v. 321, p. 612-614, 2000.

CFM - CONSELHO FEDERAL DE MEDICINA. **Resolução n° 1098, de 30 de junho de 1983**. Adota o novo Texto da Declaração de Helsinque (Helsinque II) referente à pesquisa clínica. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/1983/1098_1983.htm. Acesso em: 16 jul. 2003.

_____ . **Resolução n° 1.246, de 08 de janeiro de 1988**. Código de Ética Médica. Disponível em: http://www.portalmedico.org.br/codigo_etica/codigo_etica.asp?portal=. Acesso em: 16 jul. 2003.

_____ . **Resolução n° 1.605, de 15 de setembro de 2000**. Dispõe sobre o sigilo médico. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2000/1605_2000.htm. Acesso em: 16 jul. 2003.

_____ . **Resolução n° 1638, de 10 de julho de 2002a**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm. Acesso em: 16 jul. 2003.

_____ . **Resolução n° 1639, de 10 de julho de 2002b**. Aprova as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", dispõe sobre tempo de guarda dos prontuários, estabelece critérios para certificação dos sistemas de informação e dá outras providências. Disponível em:http://www.portalmedico.org.br/resolucoes/cfm/2002/1639_2002.htm. Acesso em: 16 jul. 2003.

_____ . **Resolução n° 1642, de 07 de agosto de 2002c**. Disciplina o relacionamento entre os médicos e empresas que atuam sob a forma de prestação direta ou intermediação de serviços médicos. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2002/1642_2002.htm. Acesso em: 16 jul. 2003.

_____ . **Resolução n° 1643, de 07 de agosto de 2002d**. Define e disciplina a prestação de serviços através da Telemedicina. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2002/1643_2002.htm. Acesso em: 16 jul. 2003.

CIHR - CANADIAN INSTITUTES OF HEALTH RESEARCH. **Selected International Legal Norms on the Protection of Personal Information in Health Research**. Ottawa: Public Works and Government Services Canada, 2001.

DENLEY, I.; SMITH, S.W. Privacy in clinical information systems in secondary care**.** **British Medical Journal**, v. 318, p. 1328-1331, 1999.

DICK, R.S.; STEEN, E.B.; DETMER, D.E. (Ed.). **The Computer-Based Patient Record**. Revised Edition, Washington, D.C.: National Academy Press, 1997.

GOSTIN, L. Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations. **Annals of Internal Medicine**, v. 127, p. 683-690, 1997.

MANDL, K.D.; SZOLOVITS, P.; KOHANE, I.S. Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private. **British Medical Journal**, v. 322, p. 283-286, 2001.

MANNING, D. Commentary: Don't waive consent lightly – involve the public. **British Medical Journal**, v. 324, p. 1213, 2002.

MS - MINISTÉRIO DA SAÚDE**. Cartão Nacional de Saúde**. [1996]. Disponível em http://dtr2001.saude.gov.br/cartao/. Acessado em: 16 jul 2003.

_____ . **Portaria nº 3.947/GM, de 25 de novembro de 1998**. Diário Oficial da União, nº 9-E, 14 jan 1999, Seção 1, pág. 8

RIND, D.M.; KOHANE, I.S.; SZOLOVITS, P.; SAFRAN, C.; CHUEH, H.C.; BARNETT, G.O. Maintaining the Confidentiality of Medical Records Shared over the Internet and the World Wide Web. **Annals of Internal Medicine**, v. 127, p. 138-141, 1997.

SBIS - SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE, Grupo de Trabalho de Certificação de Software. 2002. Disponível em: http://www.sbis.org.br/certificacao.htm. Acesso em: 15 jul. 2003.

SHORTLIFFE, E.H. The Evolution of Health-Care Records in the Era of the Internet. **Proceedings of MEDINFO98**, Semi-Plenary 2, Amsterdam: IOS Press, 1998.

STROBL, J.; CAVE, E.; WALLEY, T. Data protection legislation: interpretation and barriers to research. **British Medical Journal**, v. 321, p. 890-892, 2000.

VERITY, C.; NICOLL, A. Consent, Confidentiality, and the threat to public health surveillance. **British Medical Journal**, v. 324, p. 1210-1213, 2002.

VIANA, A.L.D.; GERSCHMAN, S.; IBAÑEZ, N.; PARADA, R. A regulamentação da Assistência Médica Suplementar no Brasil**. Nota Técnica 3, em Modelos de Regulação e Análise do Caso Brasileiro.** 2001. Disponível em: http://www.ans.gov.br/portal/site/forum_saude/forum_bibliografia_objeto_reg.asp. Acesso em: 02 jul. 2003

WILLISON, D.J.; KESHAVJEE, K.; NAIR, K.; GOLDSMITH, C.; HOLBROOK, A.M. FOR THE COMPETE INVESTIGATORS. Patient consent preferences for research use of information in electronic medical records: interview and survey data. **British Medical Journal**, v.326, p. 373-377, 2003.

Apêndice

Termos Técnicos

Acesso a ativos: uma organização ou indivíduos permite o acesso de terceiros a seus ativos de informações para quem precisar fazer uso dos mesmos no desenvolvimento de suas atividades.

Auditoria: capacidade de um sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

Autenticação – capacidade de garantir que um usuário, sistema ou informação é mesmo quem ou o que alegar ser.

Criptografia – processo pelo qual uma mensagem (o texto limpo) é transformada em uma segunda mensagem (o texto cifrado) usando uma função complexa (o algoritmo de criptografia) e uma chave criptográfica especial.

Confidencialidade: capacidade de um sistema de impedir que usuários não-autorizados vejam determinada informação, ao mesmo tempo em que usuários autorizados possam acessá-la.

Controle de acesso: é exercido pela Administração de Segurança. As atribuições de controle de acesso podem ser delegadas para administradores setoriais e locais, para a administração de determinado domínio organizacional ou de recursos.

Custódia: define-se a custódia como a responsabilidade de se guardar um ativo para terceiros; entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.

Decifragem – o processo inverso, pelo qual o texto cifrado é transformado no texto limpo, usando-se uma segunda função complexa e uma chave de decifragem. Em alguns sistemas criptográficos, a chave criptográfica e a chave de decifragem são iguais; em outros, são diferentes.

Direito de acesso: somente o proprietário do ativo, ou pessoa por ele nomeada, pode autorizar acesso ao mesmo.

Direito de acesso em função da posição funcional: está ligado à posição ocupada pela pessoa dentro da organização, e não à pessoa que a ocupa.

Disponibilidade: indica a quantidade de vezes que o sistema cumpriu uma tarefa solicitada sem falhas internas sobre o número de vezes em que foi solicitado a fazer uma tarefa. A fração do tempo em que a página esteve no ar.

Identificação – processo para se determinar quem está acessando uma dada informação ou operando um dado sistema.

Integridade: atributo de uma informação que indica que esta não foi alterada ou, se foi, o foi de forma autorizada; capacidade de um sistema de impedir que uma informação seja alterada sem autorização ou, ao menos, de detectar se isso ocorreu.

Não repúdio – capacidade de um sistema de provar que um usuário executou determinada ação no sistema.

Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos;

Operadora de Plano de Assistência à Saúde: pessoa jurídica constituída sob a modalidade de sociedade civil ou comercial, cooperativa, ou entidade de autogestão, que opere produto, serviço ou contrato de que trata o plano privado de assistência à saúde.

Plano Privado de Assistência à Saúde: prestação continuada de serviços ou cobertura de custos assistenciais a preço pré ou pós estabelecido, por prazo indeterminado, com finalidade de garantir, sem limite financeiro, a assistência a saúde, pela faculdade de acesso e atendimento por profissionais de serviços de saúde, livremente escolhidos, integrantes ou não de rede credenciada, contratada ou referenciada, visando a assistência médica, hospitalar e odontológica, a ser paga integral ou parcialmente às expensas da operadora contratada, mediante reembolso e pagamento direto ao prestador;

Política de segurança: conjunto de diretrizes destinadas a regulamentar o uso seguro dos ativos de informações de uma organização.

Propriedade de ativos: os ativos de informações da organização pertencem à mesma.

Validade do direito de acesso: o direito de acesso somente é válido para os fins para os quais foi solicitado.