Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

ESCOLA NACIONAL DE SAÚDE PÚBLICA
SERGIO AROUCA
ENSP

"A segurança das informações em saúde sob responsabilidade do DATASUS: Uma Análise com enfoque na Privacidade e na Confidencialidade"

por

Mauricio de Souza Rosario

Dissertação apresentada com vistas à obtenção do título de Mestre Modalidade Profissional em Saúde Pública.

Orientadora: Prof.ª Dr.ª Ilara Hämmerli Sozzi de Moraes
Assistente da orientadora: Prof.ª Deise de Araujo Grigório

Rio de Janeiro, novembro de 2010.

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

ESCOLA NACIONAL DE SAÚDE PÚBLICA
SERGIO AROUCA
ENSP

Esta dissertação, intitulada

"A segurança das informações em saúde sob responsabilidade do DATASUS: uma análise com enfoque na privacidade e na confidencialidade"

apresentada por

Mauricio de Souza Rosario

foi avaliada pela Banca Examinadora composta pelos seguintes membros:

Prof.ª Dr.ª Marisa Palacios da Cunha e Melo de Almeida Rego

Prof. Dr. Sergio Tavares de Almeida Rego

Prof.ª Dr.ª Ilara Hämmerli Sozzi de Moraes – Orientadora

Dissertação defendida e aprovada em 04 de novembro de 2010.

Catalogação na fonte
Instituto de Comunicação e Informação Científica e Tecnológica
Biblioteca de Saúde Pública

R789 Rosario, Mauricio de Souza
A segurança das informações em saúde sob responsabilidade do DATASUS: uma análise com enfoque na privacidade e na confidencialidade. / Mauricio de Souza Rosario. Rio de Janeiro: s.n., 2010.
99 f., graf.

Orientador: Moraes, Ilara Hämmerli Sozzi de
Grigório, Deise de Araujo
Dissertação (Mestrado) – Escola Nacional de Saúde Pública Sergio Arouca, Rio de Janeiro, 2010

1. Sistemas de Informação. 2. Comunicação Sigilosa. 3. Privacidade. 4. Consentimento Livre e Esclarecido. 5. Sistemas Computadorizados de Registros Médicos. 6. Segurança (computação). I. Título.
CDD - 22.ed. – 362.1

Ao querido Professor Doutor Miguel Murat Vasconcellos (in memorian), pela confiança depositada na segunda turma do Mestrado Profissional em Gestão da Informação e Comunicação em Saúde.

"Falar é completamente fácil, quando se têm palavras em mente que expressem sua opinião. Difícil é expressar por gestos e atitudes o que realmente queremos dizer, o quanto queremos dizer, antes que a pessoa se vá" - Carlos Drummond de Andrade.

Agradecimentos

À minha esposa Ana Rosa Pais Ribeiro, que com o seu amor, apoio e confiança foi uma força em meus despóticos dias de trabalho nesta dissertação.

Aos meus queridos filhos: Lívia Ribeiro Rosario, Renato Ribeiro Rosario e André Ribeiro Rosario.

A Professora Doutora e Orientadora Ilara Hämmerli Sozzi de Moraes por sua compreensão e inestimáveis contribuições.

A Professora e Orientadora Deise de Araujo Grigório pela preciosa ajuda.

Aos companheiros de Mestrado, especialmente, Marcos e Rosana, que sempre se preocuparam com os rumos do meu trabalho.

Ao DATASUS pela oportunidade.

À ENSP pela ajuda indispensável para a realização deste trabalho.

"Tudo quanto veja ou ouça, profissional ou privadamente, que se refira à intimidade humana e não deva ser divulgado, eu manterei em segredo e contarei a ninguém" - Hipócrates.

RESUMO

O Departamento de Informática do Sistema Único de Saúde (DATASUS), como órgão nacional responsável pela captação, processamento, controle e disseminação de informações para o Sistema Único de Saúde (SUS), mantém sob sua estrutura de Tecnologia da Informação um patrimônio em dados institucionais e sociais de altíssimo valor - bases de dados em saúde com identificação nominal da população brasileira. Em função disto, tais informações requerem que os sistemas de informática sejam protegidos contra a invasão e modificação desautorizada, evidenciando a necessidade de implantação de uma Política de Segurança da Informação. Esta pesquisa está focada nas preocupações específicas com a privacidade e a confidencialidade das informações em saúde dos pacientes-cidadãos. A linha tênue entre o compromisso de sigilo e a permissão de acesso daqueles que estão comprometidos com a utilização das informações em saúde norteou o desenvolvimento do presente trabalho.

Buscou-se, inicialmente, estabelecer as competências do DATASUS e identificar os controversos conceitos de sistemas de informação em saúde e em segurança das informações em saúde, subsídio para o levantamento bibliográfico empreendido nas principais bases de informação científica da área de Saúde, da Ciência da Informação e da Ciência da Computação. A pesquisa buscou investigar as aplicabilidades da privacidade, da confidencialidade e do consentimento esclarecido às bases de dados, bem como as exceções e as circunstâncias nas quais se justificaria a revelação, não autorizada, das informações confiadas na especial relação existente entre médico e paciente, no âmbito dos sistemas de informações sob a responsabilidade do DATASUS.

Palavras-chave: sistemas de informação, confidencialidade, privacidade, consentimento esclarecido, prontuário do paciente e segurança da informação.

ABSTRACT

The Information Technology Department of the Brazilian Unified Health System (DATASUS), as the national organization responsible for capturing, processing, control and dissemination of data to the Unified Health System (SUS), maintains under its Information Technology structure a valuable asset in terms of institutional and social data - health databases with individual identification and information of the brazilian population. Because of this, such information requires computer systems to be protected against intrusion and unauthorized modification, emphasizing the need to implement an Information Security Policy. This research focuses on specific concerns about privacy and confidentiality of health information of patients-citizens. The fine line between a commitment to confidentiality and access permission of those who are committed to the use of health information guided the development of this work.

We sought to initially establish DATASUS powers and identify controversial concepts of information systems in health and safety of health information as inputs for the survey undertaken in major bibliographic databases of scientific information on Health, Science Information and Computer Science. The research sought to investigate the applicability of privacy, confidentiality and informed consent to databases, as well as the exceptions and the circumstances in which non authorized disclosure of information entrusted in the special relationship between doctor and patient would be justified, in the scope of the information systems under the responsibility of DATASUS.

Key words: information systems, confidentiality, privacy, informed consent, medical records systems computerized e computer security.

Sumário

1. Introdução.

Esta dissertação tem por objetivo analisar a expressão dos conceitos da privacidade e confidencialidade para o contexto dos Registros Eletrônicos em Saúde (RES) que estão sob a responsabilidade do Departamento de Informática do Sistema Único de Saúde - DATASUS. Com isso, pretende contribuir para o Projeto de Classificação das Informações, oferecendo aos classificadores/gestores das informações, deste departamento, análise de aspectos técnicos e legais estabelecidos pela norma ABNT NBR ISO/IEC 17799 [1], adotada em sua Política de Segurança da Informação e Comunicações (PSIC), com ênfase naqueles aspectos que protegem os direitos dos cidadãos, relacionados à confidencialidade e à privacidade de suas informações em saúde.

Para Kobayashi e Furuie [2],

> "A área da segurança da informação em saúde ainda é bastante incipiente, permitindo pesquisas maiores e mais aprofundadas. Em particular, praticamente não há pesquisa nesta área dentro do Brasil, o que a torna uma linha promissora tanto em termos acadêmicos quanto em termos de mercado".

Considerando que este é um campo de estudo novo e que ainda existe pouca literatura que trate do assunto, optou-se por utilizar os conceitos e o referencial teórico desenvolvidos por Kobayashi e Furuie [2], em 2007, em seu artigo para a Revista de Engenharia Biomédica. O referido trabalho também fundamenta o roteiro de pesquisa adotado, para a busca de aspectos da privacidade e confidencialidade das informações em saúde, aplicáveis aos dados e às informações dos Sistemas de Informações em Saúde do DATASUS.

> "Todos os atores envolvidos no contexto da informação em saúde devem aplicar adequadamente as políticas, procedimentos e mecanismos tecnológicos de segurança para que as informações sejam acessadas e manipuladas de forma controlada" [2].

A falta de segurança permite diferentes níveis de quebra do sigilo. Francisconi e Goldim [3] definem que:

> "Podemos fazer a distinção entre quebra de privacidade e quebra de confidencialidade: a primeira consiste no acesso desnecessário ou uso de

> informações sem a devida autorização do paciente; a segunda é a ação de revelar ou deixar revelar informações fornecidas em confiança".

Também é importante considerar que a arquitetura dos bancos de dados digitais tem como característica, intrínseca à sua natureza, a noção de conectividade. Ao permitir o acesso remoto a grandes quantidades de informação, facilita-se a referência cruzada das informações, a qual, no caso dos bancos de dados em saúde, colocam em perigo a confidencialidade dos dados do paciente.

Para D'Ornellas e Rocha [4]:

> "A combinação de dados a partir de sistemas distintos produz a síntese de novos conjuntos de dados. Este processo de agregação da informação produz sério risco de perda da confidencialidade uma vez que uma das características dos sistemas biológicos é o seu grau elevado de inter-relacionamento. Em outras palavras, é possível inferir sobre fatos importantes em um banco de dados através das informações disponíveis em outro. Além do mais, é possível que alguém, com qualquer nível de acesso a um banco de dados médico, obtenha informação altamente confidencial através de inferências a respeito de informações não-confidenciais".

Configura-se, assim, mais um objetivo a ser abordado nesta dissertação: contribuir para que as informações em saúde sejam utilizadas, de forma segura, em prol do bem estar dos cidadãos, mantendo-as disponíveis e acessíveis para que os profissionais de saúde possam desenvolver suas atividades e as instâncias governamentais possam atuar na formulação de políticas de saúde e assim como a população, através de seus representantes, possa exercer o controle social do Sistema Único de Saúde (SUS).

Em 1997, Rindfleisch [5] expressa preocupação com a segurança da informação em saúde, pois, "a segurança é vital para prover duas qualidades fundamentais em informações em saúde: a confiança e a privacidade. Sem isso, haverá conseqüências sérias". Corre-se o risco de que os pacientes passem a evitar a utilização dos serviços de saúde e também que os clínicos possam se negar a preencher todas as informações acerca do paciente. "Além disso, a existência de informações incompletas ou ainda incorretas se reflete de forma profundamente negativa na pesquisa médica, uma vez que dados incorretos levam, naturalmente, a resultados incorretos" [6].

Esta linha tênue entre o sigilo, aqui usado com amplo espectro semântico abarcando a confidencialidade e a privacidade, e a permissão de acesso aos que estão comprometidos com a utilização das informações em saúde, preservando-as daqueles que sem qualquer

preocupação e responsabilidade com essa segurança possam comprometer seu ciclo (armazenamento, recuperação, manipulação ou processamento), permeia o desenvolvimento do presente estudo. Trabalha-se, então, com a preocupação de que estejam resguardadas tanto as relações entre médico e paciente, quanto a que se estabelece entre o paciente e os entes governamentais, a partir do armazenamento dessas informações.

Portanto, a relevância desse estudo está estabelecida na medida em que pretende colaborar com a melhoria dos mecanismos que asseguram a confidencialidade e a privacidade das informações em saúde, salvaguardando a exposição desnecessária do paciente através da violação do acesso de suas informações presentes nos sistemas do DATASUS.

A competência do DATASUS como órgão nacional responsável pela captação, processamento, controle e disseminação de informações para o SUS mantém sob sua estrutura de Tecnologia da Informação um patrimônio em dados institucionais e sociais de altíssimo valor - bases de dados em saúde com identificação nominal da população brasileira. Informações consideradas “sensíveis”, que requerem a proteção contra a intrusão e modificação desautorizada, implicando na implantação de controles e processos voltados para a segurança da informação apoiada por uma Política de Segurança da Informação, no enfoque desta análise, especificamente, o olhar da privacidade e da confidencialidade.

2. Bases Teóricas e Conceituais.

2.1. O Departamento de Informática do Sistema Único de Saúde (DATASUS).

Criado pelo Decreto Nº 100 de 16 de abril de 1991, publicado no Diário Oficial da União (D.O. U.) de 17de abril de 1991 e retificado conforme publicado no D.O.U. de 19 de abril de 1991 [7], "Art. 12. Ao Departamento de Informática do SUS compete especificar, desenvolver, implantar e operar sistemas de informações relativos às atividades finalísticas do SUS, em consonância com as diretrizes do órgão setorial".

O DATASUS resulta da fusão da Diretoria de Sistemas de Saúde da Empresa de Tecnologia e Informações da Previdência Social, inicialmente denominada Empresa de Processamento de Dados da Previdência Social (DATAPREV), com setores da Fundação Serviços de Saúde Pública (Fundação SESP) e da Superintendência de Campanhas de Saúde (SUCAM). Surge como um órgão da estrutura da Fundação Nacional de Saúde (FUNASA).

De início, o conjunto de serviços consistia, basicamente, no processamento dos sistemas de informação hospitalar e ambulatorial (Sistema de Internações Hospitalares do Sistema Único de Saúde (SIH/SUS) e o Sistema de Informações Ambulatoriais do Sistema Único de Saúde (SIA/SUS)), do Sistema de Informações sobre Nascidos Vivos (SINASC), do Sistema de Informações sobre Mortalidade (SIM) e do Sistema Nacional de Agravos de Notificação (SINAN).

Atualmente, o DATASUS tem sob sua responsabilidade uma grande quantidade de informações do Sistema Único de Saúde (SUS). As informações em saúde, administrativas e as financeiras dos atuais Sistemas de Informações em Saúde (SIS), somadas às gerenciais produzidas a partir de demandas dos Gestores (Municipal, Estadual e Federal) da Saúde Pública, formam um dos seus principais ativos, ou seja, são informações relevantes para o funcionamento do SUS.

> "A informação é fundamental para a democratização da Saúde e o aprimoramento de sua gestão. A informatização das atividades do Sistema Único de Saúde (SUS), dentro de diretrizes tecnológicas adequadas, é essencial para a descentralização das atividades de saúde e viabilização do Controle Social sobre a utilização dos recursos disponíveis" [8].

"O Departamento responde de fato pela implementação do Sistema Nacional de Informação em Saúde (SNIS) do Ministério da Saúde" [9]. Apesar da amplitude de seus objetivos originais, o DATASUS vem sendo paulatinamente "esvaziado" em suas competências. Sua estrutura organizacional também é continuamente alterada, estabelecendo-se as competências presentes na Estrutura Organizacional do Ministério da Saúde, determinadas pelo Decreto N° 4.194 de 11 de abril de 2002, e atualizadas, através do Artigo 7º, do capítulo III do Decreto nº 7135 [7], de 29 de março de 2010.

> Ao Departamento de Informática do SUS - DATASUS, órgão da Secretaria Executiva do Ministério da Saúde compete:
>
> I - fomentar, regulamentar e avaliar as ações de informatização do SUS, direcionadas para a manutenção e desenvolvimento do sistema de informações em saúde e dos sistemas internos de gestão do Ministério;
>
> II - desenvolver, pesquisar e incorporar tecnologias de informática que possibilitem a implementação de sistemas e a disseminação de informações necessárias às ações de saúde, em consonância com as diretrizes da Política Nacional de Saúde;
>
> III - manter o acervo das bases de dados necessárias ao sistema de informações em saúde e aos sistemas internos de gestão institucional;
>
> IV - assegurar aos gestores do SUS e órgãos congêneres o acesso aos serviços de informática e bases de dados mantidos pelo Ministério;
>
> V - definir programas de cooperação técnica com entidades de pesquisa e ensino para prospecção e transferência de tecnologia e metodologia de informática em saúde, sob a coordenação do Secretário-Executivo, e das atividades do SUS;
>
> VI - apoiar estados, municípios e o Distrito Federal, na informatização.

Essa vinculação do DATASUS como órgão da Secretaria Executiva do Ministério da Saúde, que tem por objetivo permitir o uso das informações em saúde como ferramenta fundamental para apoio à gestão do SUS, deveria implicar automaticamente a ampliação e a modernização de sua área de tecnologia da informação.

Ao longo de sua história, observam-se marcos importantes como o documento enviado ao DATASUS pela Organização Mundial de Saúde – OMS e pela Organização Pan-Americana de Saúde – OPAS, considerando que "... o conjunto de informações sobre saúde hoje disponível [pelo DATASUS] é um dos mais completos existentes no mundo" [10].

Fundamentando-se, dessa forma, a afirmativa que: "... o DATASUS está hoje entre as principais instituições de Tecnologia da Informação do Governo Federal, e tem talvez a melhor das estruturas de informática entre todos os órgãos da administração direta" [10].

Observa-se, entretanto, que ainda há muito a ser construído ao adotar-se como referência o contido no documento da proposta de Política Nacional de Informações e Informática em Saúde (PNISS), de março de 2004 [11], na busca de estabelecer a estratégia da PNIIS para os usos da informação em saúde e as responsabilidades institucionais do DATASUS.

> **Propósito**
>
> Promover o uso inovador, criativo e transformador da tecnologia da informação, para melhorar os processos de trabalho em saúde, resultando em um Sistema Nacional de Informação em Saúde articulado, que produza informações para os cidadãos, a gestão, a prática profissional, a geração de conhecimento e o controle social, garantindo ganhos de eficiência e qualidade mensuráveis através da ampliação de acesso, eqüidade, integralidade e humanização dos serviços e, assim, contribuindo para a melhoria da situação de saúde da população.

A macro-função estratégica de gestão para as três esferas de governo, estabelecida implicitamente para a área de Informação e Informática em Saúde neste propósito, define o papel do DATASUS de "garantir, nas três esferas de governo, com definição de prazos, a compatibilização, interface e modernização dos sistemas de informação do SUS e o aperfeiçoamento da integração e articulação com os sistemas e bases de dados de interesse para a saúde" [11].

Delineia-se, desta forma, a complexidade para a elaboração e implementação de uma política de segurança da informação com a preocupação de manter a integridade, confidencialidade e disponibilidade das informações em saúde sob a responsabilidade do DATASUS.

2.1.1 Os Sistemas de Informação em Saúde.

É importante considerar a trajetória da Informação e Comunicação na área da saúde (Informática em Saúde), impulsionadas pela Tecnologia da Informação, "que teve o seu reconhecimento nacional a partir do I Seminário em Informática em Saúde, iniciativa do Ministério da Saúde, base para a criação, em 1986, da Sociedade Brasileira de Informática em Saúde (SBIS)" [12].

No escopo deste trabalho, adota-se o conceito para a Informática Médica ou Informática em Saúde (em Inglês, *Medical Informatics*), de acordo com esta sociedade, que o define como, "... um campo de rápido desenvolvimento científico que lida com armazenamento, recuperação e uso da informação, dados e conhecimentos biomédicos para a resolução de problemas e tomada de decisão" [13].

Para a SBIS [13],

> "A Saúde é uma das áreas onde há maior necessidade de informação para a tomada de decisões. A Informática Médica é o campo científico que lida com recursos, dispositivos e métodos para otimizar o armazenamento, recuperação e gerenciamento de informações biomédicas. O crescimento da Informática Médica como uma disciplina deve-se, em grande parte: aos avanços nas tecnologias de computação e comunicação, à crescente convicção de que o conhecimento médico e as informações sobre os pacientes são ingerenciáveis por métodos tradicionais baseados em papel, e devido à certeza de que os processos de acesso ao conhecimento e tomada de decisão desempenham papel central na Medicina moderna".

São as seguintes áreas de atuação da Informática em Saúde: "Sistemas de Informação em Saúde, Prontuário Eletrônico do Paciente, Telemedicina, Sistemas de Apoio à Decisão, Processamento de sinais biológicos, Processamento de Imagens Médicas Internet em Saúde, Padronização da Informação em Saúde" [13].

A história dos Sistemas de Informações em Saúde (SIS) gerenciados pelo DATASUS pode ser contada a partir da herança dos sistemas oriundos da Empresa de Processamentos de Dados do Ministério da Previdência Social - DATAPREV, ferramentas para as ações em saúde e de controle contábil-financeiro do faturamento assistencial médico-hospitalar e ambulatorial:

- Sistema de Assistência Médico-Hospitalar da Previdência Social (SAMHPS), mais conhecido como o Sistema da Autorização de Internação Hospitalar (AIH);
- Sistema Guia de Autorização de Pagamentos (GAP);
- Sistema de Informações e Controle Ambulatorial da Previdência Social (SICAPS).

Apesar de possuírem um escopo mais amplo, o principal uso destes sistemas, foi controlar o pagamento dos serviços prestados pelos hospitais contratados pelo Instituto Nacional de Assistência Médica da Previdência Social (INAMPS), autarquia federal com sede em Brasília (DF), criado pela Lei n° 6.439 [7], de 1° de setembro de 1977, e vinculado

ao Ministério da Saúde pelo Decreto n° 99.060 [7], de 7 de março de 1990 e extinto em 27 de julho de 1993 pela Lei nº 8.689 [7].

Na verdade, estes sistemas controlavam somente os atendimentos médicos para os que contribuíam para a previdência social, sendo a maior parte realizada pela iniciativa privada através de convênios. A remuneração desses contratos e convênios por procedimentos consolidou, "a prática de cuidar da doença e não da saúde, expressa na lógica organizativa dos principais Sistemas de Informações em Saúde (SIS)" [14] herdados pelo DATASUS.

Além dos sistemas já citados, também fazem parte da história dos SIS do DATASUS, os de origem no Ministério da Saúde e de características epidemiológica:

- Sistema de Informações sobre Mortalidade (SIM);
- Sistema de Informações sobre Nascidos Vivos (SINASC);
- Sistema de Informação de Agravos de Notificação (SINAN);

A descentralização dos serviços de saúde, por força da implantação do Sistema Único de Saúde (SUS), a partir da Constituição Federal de 1988 [7], na proposta do capítulo II específico sobre Seguridade Social e consolidada pela Lei Orgânica da Saúde (LOS 8.080) [7], que substituiu o conceito de cobertura ao contribuinte, pela cobertura ao cidadão, buscou recuperar uma imensa dívida social com uma grande parcela da população brasileira, avançando na direção de uma sociedade mais justa, onde os direitos sociais não estariam vinculados a contribuições anteriores.

> "Existe um consenso nacional de que uma política substantiva de descentralização tendo como foco o município, que venha acompanhada de abertura de espaço para o controle social e a montagem de um sistema de informação que permita ao Estado exercer seu papel regulatório, em particular para gerar ações com capacidade de discriminação positiva, é o caminho para superar as causas que colocam o Serviço Único de Saúde (SUS) em xeque" [15].

A força dessa descentralização influencia na configuração, organização e acesso ao SUS, no qual o Estado tem suas funções e suas responsabilidades redefinidas pelo aprovisionamento e gestão de atenção à saúde, evidenciadas na expressão constitucional "a saúde é direito de todos e dever do Estado", passando a ser o principal ator na garantia de acesso aos serviços de saúde para todos os cidadãos. A complexidade deste novo sistema de

saúde brasileiro impacta diretamente os atuais SIS, objetivando atender essa nova composição do SUS.

> "Compõem obrigatoriamente os sistemas de gerência em saúde, os sistemas informativos da condição do doente, de sua vida, do meio ambiente e de outros fatores que interferem no processo saúde-doença e que constituem os Sistemas de Informação em Saúde (SIS)" [15].

A necessidade por informação específica e regionalizada, a dicotomia entre ações curativas e as de promoção de saúde, bem como um modelo de financiamento ainda baseado no pagamento de procedimentos/produção, definem uma arquitetura com diversos sistemas de informação, formadores de bases de dados nacionais: uma lógica fragmentadora, sem a preocupação com a interoperabilidade[*] dos serviços e das informações dos sistemas, "conseqüência da falta de padrões para representar essas informações gerando retrabalho na coleta dos dados; visões fragmentadas das informações em saúde necessárias e bases de dados com baixa confiabilidade" [16].

> "Essa especificidade exige para o desenho e implementação dos *SIS* uma clara fundamentação clínica e epidemiológica em planejamento, programação e avaliação em saúde, além dos conhecimentos em *SI* e *TI*. Isso porque esses sistemas deverão informar sobre a doença dos indivíduos e seu perfil na comunidade, sobre as causas e condições que propiciam o aparecimento delas, sobre a atividade clínica, condutas, normas técnicas, tecnologias em saúde utilizadas, ações programáticas e resultados, como extensão e impacto das ações na população ou grupos de risco. Assim, a construção de Sistemas de Informação em saúde requer equipe multiprofissional, para onde confluam os vários saberes técnicos para essa confecção, sendo fundamental a opinião dos profissionais usuários" [15].

O Projeto do Cartão Nacional de Saúde, cuja importância já era identificada na Norma de Operação Básica do SUS de 1996, NOB SUS 96 [17], publicada no D.O.U. de 6/11/1996, documento que visou o aperfeiçoamento da gestão dos serviços de saúde e a

---

[*] Interoperabilidade não é somente integração de sistemas nem somente integração de redes. Não referencia unicamente troca de dados entre sistemas e não contempla simplesmente definição de tecnologia.

É, na verdade, a soma de todos esses fatores, considerando, também, a existência de um legado de sistemas, de plataformas de hardware e software instaladas. Parte de princípios que tratam da diversidade de componentes, com a utilização de produtos diversos de fornecedores distintos. Tem por meta a consideração de todos os fatores para que os sistemas possam atuar cooperativamente, fixando as normas, as políticas e os padrões necessários para consecução desses objetivos.

http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/o-que-e-interoperabilidade

própria organização do SUS em âmbito nacional, dentre outras orientações para a nova formulação dos sistemas municipais, propunha uma solução para a necessidade de integração e a articulação dos serviços de saúde, "a instituição do cartão SUS-MUNICIPAL, com numeração nacional, de modo a identificar o cidadão com o seu sistema e agregá-lo ao sistema nacional. Essa numeração possibilita uma melhor referência intermunicipal...".

Em seu projeto original iniciado em meados de 1999, "através de uma licitação internacional para contratação da Solução de Informática do Cartão Nacional de Saúde, financiado pelo Banco Interamericano de Desenvolvimento (BID)" [18], o sistema foi implantado, em 44 municípios, localizados em 11 estados, abrangendo cerca de 13 milhões de habitantes. A escolha privilegiou desde pequenas cidades a grandes centros urbanos, com serviços de alta complexidade, permitindo sua operação nos três níveis de governo para avaliação de aspectos conceituais e operacionais.

A identificação individualizada dos usuários relacionada ao seu município de residência, mas de abrangência nacional, característica fundamental do Sistema do Cartão Nacional de Saúde (SCNS), tem como principal objetivo vincular o atendimento realizado ao usuário, com o profissional e à unidade de saúde do atendimento. "O Cartão Nacional de Saúde é um instrumento que possibilita a vinculação dos procedimentos executados no âmbito do Sistema Único de Saúde (SUS) ao usuário, ao profissional que os realizou e também à unidade de saúde onde foram realizados" [19].

> "O Projeto Cartão Nacional de Saúde, cuja concepção, desenvolvimento e implantação são orientados pelo arcabouço que conforma o SUS, tem sido entendido como um instrumento fundamental para articular a execução descentralizada dos serviços e o caráter nacional e único do sistema de saúde. A contribuição do Cartão na integração entre o local e o nacional é dada pela captura de informações no ato do atendimento prestado ao usuário e o acompanhamento do seu fluxo subseqüente, em cada contato deste usuário com o SUS, em qualquer localidade do país" [16].

A coleta da informação, assim estruturada, visa a contribuir para a organização e planejamento (gestão) dos serviços de saúde e a facilitar o acesso dos usuários aos serviços do SUS. O processamento distribuído e em camadas, os padrões abertos e públicos e a identificação única do usuário, do profissional de saúde e do estabelecimento de saúde, impõem definições de padrões para se estabelecer a integração e a interoperabilidade entre

os diferentes sistemas, na direção da construção de um Sistema Nacional de Informação em Saúde (SNIS).

> "Os princípios de universalidade de acesso, integralidade de atendimento, eqüidade, democratização e descentralização do SUS, bem como o direito do cidadão à preservação de sua autonomia, integridade moral e privacidade quanto às informações relacionadas à sua saúde, são as bases que norteiam a construção do Cartão Nacional de Saúde" [16].

Ao apoiar-se nos princípios de universalidade de acesso, integralidade de atendimento, equidade, democratização e descentralização do SUS, evidencia-se a necessidade de ações e políticas visando à segurança dessas informações, agora, nacionalmente identificadas, possivelmente centralizadas (âmbitos federal, estadual e municipal) e suscetíveis a diversos tipos de ameaças à privacidade e à confidencialidade, inerentes a sua natureza altamente sensível.

2.1.2 Registros Eletrônicos em Saúde e Prontuário Eletrônico do Paciente.

A conectividade e a integração entre sistemas de informação em saúde, embutidas na concepção do Sistema do Cartão Nacional de Saúde, estabelecem a necessidade de interoperabilidade dos sistemas de informação em saúde e, consequentemente, favorece o desenvolvimento do Prontuário Eletrônico do Paciente (PEP).

> "Atualmente, o conjunto de dados capturado no registro do atendimento pelo projeto do Cartão Nacional de Saúde constitui o principal marco referencial de padrões na área de informação em saúde no País e abre novas perspectivas para o País com a construção do repositório nacional de registros clínicos" [20].

A conectividade e a integração entre sistemas de informação, presente na troca de informações em saúde, proporcionadas pela identificação individualizada dos usuários do SUS (paciente, profissionais e estabelecimentos) estabelecem, também, aspectos de risco e de vulnerabilidade, que ameaçam a segurança do repositório de registros clínicos, colocando a eficiência e a interoperabilidade de um lado, e a confidencialidade e a privacidade, do outro, na balança da segurança das informações em saúde.

No Edital de Licitação do Sistema do Cartão Nacional de Saúde [18], constava como uma das principais diretrizes que:

> "... quaisquer informações identificadoras ou diretamente correlacionáveis com os usuários, decorrentes da utilização do Cartão, serão consideradas confidenciais e sujeitas às mesmas normas éticas que regulam o acesso aos prontuários médicos e o seu uso, bem como a sanções legais, civis, administrativas e penais se comprovada a quebra de sigilo".

O Prontuário do Paciente, em papel ou eletrônico, possui várias denominações: Prontuário do Paciente, Prontuário Médico, Registro do Paciente, Prontuário Médico do Paciente etc. Diversas traduções foram encontradas para a expressão *Electronic Health Records*, abreviada como EHR, sendo que Registros Eletrônicos em Saúde (RES) ou Prontuário Eletrônico de Paciente (PEP) são, efetivamente, as mais usuais.

Segundo Roger e Gaunt [21], independentemente da denominação utilizada, o prontuário do paciente é "uma memória escrita das informações clínicas, biológicas, diagnósticos e terapêuticas de uma pessoa às vezes individual e coletiva, constantemente atualizado".

De uma forma bem simples, os Registros Eletrônicos em Saúde (RES) fazem parte dos atuais Sistemas de Informação em Saúde (SIS) e são gerados e mantidos dentro dos Estabelecimentos Assistenciais de Saúde - EAS (hospital, uma clínica, o consultório de um clínico geral etc.). Denominam-se Prontuários Eletrônicos do Paciente (PEP) se fizerem parte de um Sistema de Informações em Saúde, "compondo um conjunto de informações multi-profissionais e multi-institucionais sistematizadas (uma rede integrada de serviços clínicos) a respeito de cuidados médicos, exames, diagnósticos, tratamentos e evolução clínica, ao longo da vida do paciente" [20].

O PEP é um registro longitudinal dos cuidados fornecidos ao paciente em qualquer lugar, ao longo do tempo. É gerado a partir dos registros dos atendimentos em qualquer cenário envolvendo o fornecimento de cuidados em saúde e deve contemplar dados demográficos do paciente, diagnósticos, medicações, evolução dos tratamentos, sinais vitais, histórico clínico passado (hereditariedade), imunizações, dados laboratoriais, relatórios de radiologia etc.

> "Prontuário do Paciente é um documento único constituído por um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência, a ele prestada, de caráter legal, sigiloso e científico, utilizado para possibilitar a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo" [22].

A preocupação do MS em integrar sistemas e bases de dados de interesse para a saúde introduziu a importância da interoperabilidade entre sistemas de informações em saúde. Para Leão [23], "interoperabilidade é a capacidade de se comunicar em sistemas de informação independentes e heterogêneos, com a finalidade de promover uma rede de comunicação...".

> "A aplicação do PEP implica, necessariamente, a adoção de padrões na representação da informação (vocabulário), dos meios de armazenamento (hardware e software), bem como ao que se refere a telecomunicações (transmissão e acesso) e padrões de segurança da informação em saúde. O uso de padrões viabiliza a troca de dados e de textos livres, possibilitando a automação dos processos (assistencial, administrativo, de pesquisa, ensino e da gestão de um sistema de saúde)" [20].

O potencial de padronização e de automatização transforma o PEP em uma verdadeira ferramenta de organização da produção e de registro dos serviços de saúde, "ao coletar e armazenar o conjunto de dados necessários do atendimento em saúde, o PEP registra a informação necessária para recuperar os dados do atendimento para quaisquer fins: clínico, jurídico, administrativo e de pesquisa" [20].

> ".... a tecnologia não é o problema para se fazer a integração e promover a interoperabilidade de sistemas de saúde e sim, a solução. ... a internet e seu alto poder de conectividade permite instituições geograficamente distantes compartilhar dados clínicos com todos os usuários de serviços de saúde. ... os softwares de navegação na Internet, pela facilidade de acesso a informação presente na world wide web (www) permitem a busca, a pesquisa e a transferência de informação da rede para o microcomputador pessoal de forma rápida e eficiente" [20].

Tendo em vista que os dados possuem a identificação dos usuários do sistema de saúde, e que regras muito rígidas a respeito da segurança das informações foram definidas, estabeleceram-se os aspectos tecnológicos necessários para o PEP contribuir com a interoperabilidade entre os Sistemas de Informações em Saúde do SUS (SIM, SINASC, SINAN, SIH/SUS, SIA/SUS etc.) e a preservação do sigilo, da privacidade, da confidencialidade, da autenticidade e da integridade dos dados em saúde.

O Conselho Federal de Medicina (CFM), empenhado em manter seu protagonismo no contexto legal e ético do prontuário do paciente, e, extrapolando suas funções, aprovou a resolução nº 1331/89 [22] que trata da temporalidade do PEP, e as portarias nº 1638/2002 e nº 1821/2007 [22], que normalizam tanto o uso de sistemas informatizados, quanto a guarda e o

manuseio de prontuários. Ficaram assim definidos os aspectos jurídico-institucionais – autenticidade, integridade, confidencialidade, privacidade, confiabilidade, auditagem, assinatura eletrônica e guarda de documentos – visando a estabelecer as normas de segurança da informação do PEP.

2.1.3 Sistema de Gerenciamento de Informações Locais (GIL).

O Sistema Gerenciamento de Informações Locais (GIL) é um sistema que se destina à informatização da rede ambulatorial básica do SUS. Tem como principal objetivo servir de subsídio para os gestores locais identificarem as necessidades peculiares de sua população alvo, auxiliando, assim, a execução das ações e os serviços da Atenção Básica em Saúde.

> "Nesta última década, a Atenção Básica foi gradualmente se fortalecendo como condição necessária para a estruturação dos sistemas locais de saúde e para a efetiva consolidação dos princípios e diretrizes do SUS. Dezenas de documentos e portarias foram publicadas com objetivo de orientar a organização e a execução da Atenção Básica, do Programa de Saúde da Família (PSF) e também do Programa de Agentes Comunitários de Saúde (PACS), o que resultou em expressiva fragmentação normativa, comprometendo a própria compreensão do tema em todas as instâncias de gestão do SUS" [24].

A finalidade do GIL é "sistematizar as ações no atendimento dos estabelecimentos de saúde, contribuindo para a melhoria da gestão em saúde" [25], obtidas através da integração e da articulação das informações em saúde, de acordo com as diretrizes da PNIIS* do Ministério da Saúde para organização dos serviços de atenção à saúde. O seu escopo o coloca como o principal sistema que pode vir a ser beneficiado pelos resultados das análises sobre a segurança das informações em saúde dessa dissertação, com foco na privacidade e confidencialidade.

---

* Diretrizes: 1. Fortalecer as áreas de informação e informática nas três esferas de governo, apoiando a sua organização e desenvolvimento, através de criação de mecanismos de articulação, com vistas à integração dos sistemas de informação em saúde;

2. Estabelecer Registro Eletrônico de Saúde que permita recuperar, por meios eletrônicos, as informações em saúde do indivíduo em seus diversos contatos com o sistema de saúde, com o objetivo de melhorar a qualidade dos processos de trabalho em saúde, incluindo a disponibilidade local de informações para a atenção à saúde. [11]

O GIL é uma realização da equipe de desenvolvimento de sistemas, da então, Coordenação de Sistemas de Atenção Básica (DATASUS/COSAB), e sua implantação, desde 2004, busca alcançar a otimização e a integração completa de todos os sistemas do Ministério da Saúde para área da Atenção Básica, disponibilizados pelo DATASUS. Tendo como principais objetivos a melhoria da gestão, a sistematização das ações dos estabelecimentos assistenciais de saúde e o aprimoramento da qualidade do atendimento prestado à população.

> **"**O GIL (Gerenciador de Informações Locais) destina-se à informatização da rede ambulatorial básica do Sistema Único de Saúde – SUS auxiliando na administração dos seus processos e fornecendo informações sobre a morbidade da população atendida, subsidiando os gestores nas tomadas de decisões. Permite o monitoramento e o planejamento contínuo do sistema de saúde no Município" [25].

As funcionalidades deste gerenciador incorporam os conceitos do Sistema de Gerenciamento de Unidade Ambulatorial Básica (SIGAB), do Sistema de Gerenciamento de Unidade Ambulatorial Especializada (SIGAE), do Sistema Central de Marcação de Consultas (CMC) e do Banco de Dados Nacional de Informações Ambulatoriais do SUS (BD–SIASUS), que se constituíam nos principais Sistemas de Informações em Saúde, de âmbito nacional para atenção básica, e que eram eficientes, mas não eficazes em seus recursos informacionais disponíveis para gestão das Unidades de Saúde (US).

> "Sistemas de serviços de saúde baseados em equipes da Saúde da Família (SF), com forte extensão dessas características apoiadas por sistemas de comunicação (prontuários eletrônicos, Cartão SUS) e regulação (Centrais de Marcação de Consultas e de Internação Hospitalar) que definam critérios para o fluxo de usuários dentro da rede de atenção à saúde têm capacidade de impedir a fragmentação do sistema de serviços de saúde" [24].

O GIL, além de facilitar a integração das informações e dos procedimentos com outros Sistemas de Informações da Atenção Básica, possibilita o acompanhamento das referências intermunicipais e interestaduais, isto é, o fluxo dos usuários no sistema de saúde, subsidiando o planejamento e a definição das prioridades nas ações de saúde.

Podemos destacar como principais implementações do GIL, no sentido da interoperabilidade e integração das informações e dos procedimentos dos serviços das EAS, o uso da identificação única do Sistema do Cartão Nacional de Saúde (SCNS) e a

padronização de suas tabelas internas, atendendo à Política Nacional de Informação e Informática em Saúde (PNIIS) [11], expressa na diretriz sobre implementações que visam a estabelecer, através de um processo aberto e participativo, "padrões de representação da informação em saúde, abrangendo vocabulários, conteúdos e formatos de mensagens, de maneira a permitir o intercâmbio de dados entre as instituições, a interoperabilidade entre os sistemas e a correta interpretação das informações".

A interoperabilidade e a integração implementada pelo GIL eliminam a fragmentação estabelecida pelos vários sistemas de informação existentes para a área da Atenção Básica, otimizam os processos de saúde, evita o retrabalho e proporcionam, através da mesma entrada de dados, o atendimento de demandas como:

- registro das aplicações e esquemas de vacinação, gerando as informações do Sistema de Informações do Programa Nacional de Imunizações (SI-PNI);
- cadastramento e acompanhamento de gestantes do Programa de Humanização no Pré-Natal e Nascimento, gerando as informações para o sistema SisPreNatal;
- cadastramento e acompanhamento de pacientes com Hipertensão Arterial e/ou Diabetes, gerando as informações para o sistema HiperDia;
- coleta de dados dos atendimentos realizados pelas equipes do Programa de Agentes Comunitários de Saúde e do Programa de Saúde da Família (PACS/PSF), gerando as informações para o Sistema de Informação de Atenção Básica (SIAB);
- do faturamento dos EAS, gerando as informações da produção para o Sistema de Informações Ambulatoriais do SUS (SIA/SUS).

Evitam, desta forma, "os SIS amuados", definição de Carvalheiro, em sua bela e poética contribuição, destacada, por Moraes e Gonzáles de Gómez [26], "eliminar a fragmentação em miríade de Sistemas de Informação em Saúde (SIS) amuados, que não conversam entre si, é sensato".

> "SIS amuados! Simplesmente preciosa tal afirmação! A gravidade dessa constatação é que a fragmentação dos SIS contribui para uma compreensão fragmentada dos processos de saúde/doença/cuidado com a conseqüente fragmentação das ações de saúde. Essa miríade confere uma certa 'fugacidade' à própria apreensão sistemática do que ocorre nas situações concretas da vida, como breves flashes, partes de um quebra-cabeça que não se encaixam" [26].

A necessidade da busca da segurança das informações do Sistema de Gerenciamento de Informações Locais (GIL), com o foco em privacidade e confidencialidade por parte do DATASUS, é um exemplo de sua responsabilidade com um sistema que pode ser instalado em qualquer Estabelecimento Assistencial de Saúde (EAS) da rede ambulatorial básica do SUS, ou seja, fora de seu Parque Tecnológico e não sujeitos às suas Políticas de Segurança da Informação (PSI).

No entanto, essa configuração não diminui a responsabilidade do DATASUS nas violações da privacidade e/ou de quebras de confidencialidade das informações, que possam ocorre no sistema. O fato dos bancos de dados e as aplicações não se encontrarem, totalmente, sob as normas de sua PSI, não o isenta da obrigação de responder pelos possíveis danos causados, resultantes das "lesões", nas informações privadas e confidenciais em saúde dos pacientes-cidadãos.

2.2 Segurança da Informação.

As responsabilidades atribuídas ao DATASUS, pelo Decreto nº 7135 [7], de 29 de março de 2010, que trata da Estrutura Regimental do Ministério da Saúde, de coletar, processar e disseminar as informações em saúde para a gestão e o controle social do SUS, bem como para apoio à pesquisa em saúde, impõe a implantação de procedimentos voltados para a segurança da informação, apoiados em uma Política de Segurança da Informação (PSI), que contenha normas adequadas, principalmente no que diz respeito à classificação dos níveis de proteção e segurança dessas informações. Para Wadlow [27],

> "A segurança deverá ser proporcional ao valor do que se está protegendo. Parte desse valor é realmente um valor; outra parte é o trabalho necessário para restabelecê-lo; uma outra parte mais sutil é o trabalho que permitirá confiar em sua rede novamente".

Sabendo-se que a segurança é um processo evolutivo e não um projeto rígido e fechado em função das evoluções tecnológicas, faz-se necessário um constante acompanhamento e uma atualização contínua dos mecanismos de segurança, para evitar

que esta se torne sem efeito ou, ainda pior, um fardo que impede que as tarefas sejam executadas a contento. Ratificando este pensamento, Iachello e Abowd [28], dizem que:

> "Os projetos relativos à segurança, incluindo-se os na área médica, trazem consigo o chamado Princípio da Proporcionalidade, que estabelece a necessidade de se ter um equilíbrio entre a utilidade da aplicação, sistema, ferramenta ou processo a se tornar seguro, e a segurança e privacidade das entidades envolvidas, isto é, deve-se introduzir a segurança de forma que o ônus das suas medidas não seja tão grande a ponto de tornar o sistema impraticável de ser usado".

As medidas para segurança de sistemas de informação podem estar relacionadas com equipamentos/*softwares*, com pessoal ou com os procedimentos para o funcionamento do sistema, "... é bom lembrar que o nível de segurança atingido depende do nível de confiança que se assume acerca das medidas nos níveis organizacional, pessoal e tecnológico" [29].

Tecnologicamente os conceitos como criptografia, controle de acesso e integridade dos dados, são os primeiros a serem lembrados quando se pensa em segurança da informação, embora, juntamente com as exigências legais, as avaliações de riscos para identificar as vulnerabilidades e as ameaças formem a arquitetura básica das políticas de segurança da informação, que definem os detalhes necessários para a garantia da segurança e privacidade das informações [30].

O enfoque da privacidade e da confidencialidade para as informações em saúde propostos nesta dissertação estão baseados na afirmativa de Niinimäki [31], para quem a segurança não é uma questão simplesmente tecnológica: "... a segurança é um problema em termos de pessoas, não em termos de tecnologias". Decorre daí a conclusão de que não existe segurança total, mesmo em se tratando de informações precisas, provenientes de fontes confiáveis e acessadas apenas por pessoas autorizadas, como no caso das informações clínicas, ou seja, tecnologias de segurança da informação são necessárias, mas não são suficientes.

A ênfase na dimensão confidencialidade das informações em saúde, expressa como "... a ação de revelar ou deixar de revelar informações fornecidas em confiança" [3], deve subsidiar a Política de Segurança da Informação do DATASUS privilegiando o direito fiduciário dos pacientes e o dever dos responsáveis envolvidos em sua custódia. Considera

o suporte relacionado com a esfera da tecnologia e das ferramentas necessárias para proteção e prevenção contra o desvelar não autorizado das informações em saúde.

2.2.1 Legislação Brasileira.

A questão da segurança está incluída nas preocupações das organizações internacionais de saúde. Segundo a Organização Pan-Americana de Saúde (OPAS) [32]:

> "Os Sistemas de Informações em Saúde (SIS) armazenam dados identificados sobre saúde dos indivíduos, e essas informações são muito sensíveis. Dados médicos inserem-se na esfera mais íntima do indivíduo. Conteúdo dos prontuários pode causar danos ao paciente, se forem utilizados fora da relação médico-paciente. Divulgação não autorizada de dados pessoais médicos pode, portanto, levar a várias formas de discriminação, a incriminação, e até mesmo a violação de direitos fundamentais".

Está presente também nas ações do Governo Federal que visam assegurar a proteção da informação sob sua responsabilidade, e garantir o direito dos cidadãos de acesso (confidencial e privado) às informações de seu interesse, previsto, inicialmente, na Constituição de 1988 [7], de acordo com inciso LXXII, do artigo 5º no Capítulo I, em que determina, nas alíneas a e b, que o "hábeas-data" é a ação que garante ao interessado o acesso a informações atinentes à sua pessoa, constante de registro ou bancos de dados de entidades governamentais ou de caráter público, bem como de retificação desses dados.

A relevância da segurança é ratificada nas propostas da 12ª Conferência Nacional de Saúde [8], ganhando grande espaço no cenário nacional, atingindo as três esferas públicas de governo: federal, estadual e municipal.

> "Os gestores das três esferas de governo, em articulação com seus gestores da Área de Informação e Informática em Saúde, deverão congregar e coordenar os esforços institucionais no sentido de colocar a Informação e a Informática em Saúde a serviço do Sistema Único de Saúde – SUS".

As ações sobre a segurança das informações públicas, do Governo Federal, são regidas por diversas leis. Destacam-se, a seguir, algumas das leis promulgadas nesta década:

- Decreto Nº. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal [7];

- Decreto Nº 4.553, de 27 de dezembro de 2002, que 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 [7];

- Decreto Nº 5.772, de 8 de maio de 2006, que estabelece as competências do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República [7];

- Acórdão 461/2004 do Tribunal de Contas da União (TCU), sessão de 28 de abril de 2004 - Plenário, voto do Ministro Relator Marcos Vilaça, da auditoria para a verificação dos aspectos de segurança, qualidade e controles dos sistemas de processamento de dados do DATASUS [33].

2.2.2 Normas da Associação Brasileira de Normas Técnica.

A necessidade de integrar/interoperar sistemas implica na busca por padrões e nas melhores práticas para segurança de sistemas e informações, conseqüência direta dos problemas ocasionados por acidentes, ações de má conduta, atividades criminosas, invasões a sistemas por ações de hacker (pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros).

Das experiências obtidas com essas ações, surgem as perguntas: o que fazer para que tais ações não ocorram? E se ocorrerem, que ações deverão ser adotadas para minimizar seus impactos? Gênese dos padrões para prevenção de tais ocorrências, "Vários controles podem ser considerados como princípios orientadores que fornecem um bom ponto de partida para implementação da segurança de informações" [1].

Em 1987, o Departamento de Comércio e Indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (*Commercial Computer Security Centre*), que dentre suas atribuições tinha a tarefa de estabelecer uma norma de segurança para as informações do Reino Unido [34].

A partir de 1989, vários documentos preliminares foram publicados por esse centro, até que, em 1995, desenvolvido pelo *British Standart Institution*, surgiu o padrão BS 7799. Esse documento foi disponibilizado em duas partes para consulta pública, a primeira em

1995 (BS 7799-1:1995 *Information technology - Code of pratic for information security management*) e a segunda em 1998 (BS 7799-2:1998 *Information Security Management Systems*) [34].

> "A ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) formam o sistema especializado para padronização mundial. Entidades nacionais que são membros da ISO ou IEC participam do desenvolvimento de Padrões Internacionais através de comitês técnicos estabelecidos pela respectiva organização para lidar com campos específicos de atividade técnica. Os comitês técnicos da ISO e da IEC colaboram em campos de interesse mútuo. Outras organizações internacionais, governamentais e não-governamentais, em associação com a ISO e a IEC, também participam dos trabalhos" [1].

A seguir, em 1º de dezembro de 2000, após incorporar diversas sugestões e alterações, a BS 7799 ganhou status internacional com sua publicação na forma da ISO/IEC 17799:2000, aprovado pelo Comitê Técnico Conjunto (*Joint Technical Committee - JTC*), formado pela ISO e pelo IEC, chamado ISO/IEC JTC 1, comitê de âmbito internacional, responsável (desenvolver, manter, promover e facilitar) pelas informações relativas aos padrões de tecnologia da informação [34].

Por fim, em setembro de 2001, a Associação Brasileira de Normas Técnicas (ABNT) homologou a versão brasileira da norma, denominada NBR ISO / IEC 17799. Contemplando padrões de controles e recomendações, a serem adotados para implementar e gerenciar a segurança da informação, objetivando garantir a continuidade dos negócios e minimizar danos pela preservação da disponibilidade, integridade e confidencialidade das informações [34].

> "Acompanhando o processo apresentado de evolução histórica, pode-se observar que a norma ISO / IEC 17799, a evolução da BS 7799-1, incorporada pela ISO em 2000, também foi revisada, e ambas as normas, a ISO / IEC 27001 e a ISO / IEC 17799, foram alinhadas em 2005. O passo seguinte foi a conversão da ISO / IEC 17799:2005 em ISO 27002, ocorrida em 2007, complementando assim a família ISO / IEC 27000 que aborda aspectos mais amplos de Segurança da Informação". [34]

O padrão internacional ISO / IEC 27001, na realidade, é a evolução da BS 7799-2:2005, e seu título completo é ISO / IEC 27001:2005 – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação (SGSI) – Requisitos, "a primeira a abordar

segurança da informação com uma visão sistêmica de gestão e não somente como recomendações de instalação de controles de segurança isolados" [34].

A versão brasileira foi publicada pela ABNT, em 2006, sob o título NBR ISO / IEC 27001:2006 – Tecnologia da Informação - Técnicas de Segurança – Sistema de Gestão da Segurança da Informação – Requisitos [34].

> "Este padrão faz recomendações para a gestão da segurança de informações para uso daqueles que são responsáveis por iniciar, implementar ou manter a segurança em suas organizações. Intenciona fornecer uma base comum para o desenvolvimento de padrões de segurança organizacional e práticas eficazes de gestão de segurança de informações e fornecer confiança nos intercâmbios interorganizacionais. As recomendações deste padrão devem ser selecionadas e usadas de acordo com as leis e regulamentos aplicáveis" [1].

Uma vez que se tenha apresentado os diversos aspectos concernentes à evolução da norma NBR ISSO / IEC 27001: 2006, na qual a efetiva implementação de um Sistema de Gestão de Segurança da Informação - SGSI (ou *ISMS* em inglês) é apontada como um requisito passa-se a dissertar sobre um de seus elementos de controle e que está no cerne de atenção deste estudo: a Política de Segurança da Informação.

O estabelecimento de uma Política de Segurança da Informação visa "a prover uma orientação e apoio da direção para segurança da informação de acordo com o requisito do negócio e com as leis e regulamentações pertinentes" [34], através da definição do documento da política de segurança da informação, que deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes e da análise crítica constante desta política.

2.2.3 A Política de Segurança da Informação no DATASUS.

Decorrente do Acórdão 461/2004, do Tribunal de Contas da União [33], o DATASUS iniciou em 2004 a implantação de sua Política de Segurança da Informação e Comunicação (PSIC), de acordo com os ditames da Associação Brasileira de Normas Técnicas – ABNT, e os Padrões Internacionais definidos de acordo com as regras estabelecidas nas Diretivas dos comitês técnicos, da *International Organization for Standardization (ISO)* e da *International Electrotechnical Commission (IEC)*, elaborados pelo *British Standards Institution (BS)*.

A análise da sua infra-estrutura de Tecnologia de Informação (TI) resultou em um modelo de Gestão de Segurança da Informação que se encontra proposto na forma de um Plano Diretor de Segurança da Informação (PDSI) – DATASUS 2007/2010 [8]. Este plano tem como principal finalidade garantir a confiabilidade, integridade e disponibilidade das informações em saúde, no âmbito do Ministério da Saúde (MS).

Existem vários métodos para se proceder a essa avaliação. A abordagem técnica, no PDSI do DATASUS, está orientada a partir das Normas ABNT NBR ISO / IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistemas de Gestão da Segurança da Informação – Requisitos, padrão para gerenciamento de segurança da informação, na área de sistemas de informação em saúde.

Vale enfatizar que a norma ABNT NBR ISO / IEC 27001:2006 [1], apresenta os seguintes termos e definições para o seu propósito:

> Segurança de informações: Preservação da confidencialidade, integridade e disponibilidade das informações.
>
> - Confidencialidade: Garantir que as informações sejam acessíveis apenas para aqueles que estão autorizados a acessá-las.
> - Integridade: Salvaguardar a exatidão e a inteireza das informações e métodos de processamento.
> - Disponibilidade: Assegurar que os usuários autorizados tenham acesso às informações e aos ativos associados quando necessário.
>
> Avaliação de riscos: Avaliação das ameaças às informações e às facilidades de processamento de informações, dos impactos nas informações e nas facilidades, das vulnerabilidades das informações e facilidades, e da probabilidade de ocorrência de tais riscos.
>
> Gestão de riscos: Processo de identificar, controlar e minimizar ou eliminar os riscos de segurança que podem afetar sistemas de informações, a um custo aceitável.

Observa-se que "as fases do PDSI implementam os 11 controles de segurança, do Sistema de Gestão da Segurança da Informação (SGSI), estabelecidos no Anexo A da norma" [34]:

> Política de Segurança da Informação;
> Organizando a segurança da informação;
> Gestão de Ativos;
> Responsabilidade pelos ativos;
> Inventário dos ativos;
> Proprietário dos ativos;
> Uso aceitável dos ativos;
> Classificação da informação;
> Recomendação para classificação;
> Rótulos e tratamento da informação;

> Segurança em recursos humanos;
> Segurança física e do ambiente;
> Gerenciamento das operações e comunicações;
> Controle de acesso;
> Aquisição, desenvolvimento e manutenção de sistema de informação;
> Gestão de incidentes de segurança da informação;
> Gestão da continuidade do negócio;
> Conformidades.

O Projeto de Classificação das Informações, estágio atual do PDSI, define normas/regras para especificar os níveis de segurança das informações em saúde, baseadas em critérios de integridade, confidencialidade e disponibilidade, em cada um dos ciclos de vida (criação, manipulação, transmissão, armazenamento e descarte) das informações dos SIS sob responsabilidade do DATASUS.

Os valores diferenciados para sensibilidade (capacidade para 'melindrar') das informações (captadas, armazenadas, processadas, compartilhadas e descartadas), organizadas nas bases de dados, redes locais, serviços e sistemas, influenciam diretamente o processo de classificação para o nível de segurança das informações, que deve ser proporcional ao risco e a amplitude do dano causado pela perda, mau uso, exposição e/ou modificação da informação.

Assim como a complexidade da segurança das informações sob responsabilidade do DATASUS evidenciada, no nível heterogêneo de informatização de suas Coordenações Regionais, em alguns casos, bem abaixo das expectativas necessárias para uma política de segurança satisfatória, configura um ambiente tecnológico cujas informações, os ativos, os sistemas e as redes encontram-se, ainda, expostos a vários tipos de ameaças (fraudes, acidentes, vírus, ataques de *hackers* etc.) contra a segurança da informação.

> "... revela-se como altamente recomendável a criação de uma gerência específica de segurança, preferencialmente vinculada à direção geral do DATASUS" [33].

Baseadas nessas condições, e nas conclusões do PDSI [8], as políticas e/ou ações para a segurança "exigem a proteção, com maior ou menor rigor, da confidencialidade, integridade e disponibilidade das informações confidenciais tratadas pelo diversos sistemas e serviços informatizados", e que se utilizadas de forma indevida podem causar danos para os pacientes usuários dos SIS, e, com certeza, prejuízos para a confiabilidade e credibilidade do DATASUS e do Ministério da Saúde.

2.3 Segurança da Informação em Saúde

> "De modo geral, há um consenso sobre as vantagens dos registros eletrônicos, que evitariam a deterioração, a perda e a adulteração de histórias clínicas, a duplicação de prescrições terapêuticas e de exames, com evidente redução de custos. Também permitiriam reunir toda a informação sobre o paciente, identificando-o univocamente e preservando sua privacidade, além de armazenar informações de interconsultas" [8].

Na análise de diferentes conceitos da segurança das informações em saúde, a abordagem tem início na vulnerabilidade dos processos que antecedem aos registros nos sistemas do DATASUS. Segundo Rindfleisch [4], "as informações do paciente podem ser utilizadas por um número muito grande de pessoas das mais variadas instituições". Dessa forma, para a eficaz implantação de medidas de segurança da informação na área da saúde é necessário conhecer os possíveis caminhos que serão percorridos, seus contextos, e também que seja estabelecida uma aproximação entre os especialistas na área de saúde e os especialistas em segurança da informação, uma vez que uns possuem poucos conhecimentos da área dos outros.

A informação deve ser correta, precisa e estar disponível, a fim de ser armazenada, recuperada, manipulada ou processada, de forma a poder ser trocada de forma segura e confiável. O acesso à informação certa no tempo certo, na quantidade certa e no local certo e a existência de ferramentas de suporte à decisão colaboram para o aumento da qualidade do tratamento a que está sendo submetido o paciente. "Para tanto, existem alguns grandes desafios a serem resolvidos, incluindo-se a proteção da privacidade, confidencialidade e segurança dos dados". [35]

No contexto hodierno da saúde, a tecnologia da informação está presente em todas as atividades das unidades de saúde, com a introdução das modernas tecnologias de informação e comunicação da assistência médica, torna-se inevitável a substituição dos prontuários em papel por Registros Eletrônicos em Saúde (RES) do paciente.

O grande número de informações a serem captadas, armazenadas, processadas e gerenciadas faz emergir uma questão bastante delicada: a da segurança e da privacidade dos dados do paciente; Raghupathi e Tan [36] afirmam que "o prospecto de armazenar informações em saúde na forma eletrônica suscita discussões acerca de padrões, ética, privacidade, confidencialidade e segurança".

A introdução da rotina referente ao prontuário eletrônico do paciente (PEP) estabelece "um objeto que aglutina diversas funcionalidades centradas no atendimento direto ao paciente" [37], constituído de informações extremamente variadas e de graus diversos de complexidade, no qual pessoas e entidades de diversas áreas de atuação acessam tais informações com propósitos bastante distintos, em vários tipos de equipamentos e em sistemas também diferentes. Esta realidade implica sair do lugar comum da ênfase que tem sido dada à senha de acesso e à criptografia na defesa da privacidade e da confidencialidade nos processos de comunicação e transferência das informações.

Para Kobayashi e Furuie [2], "toda medida de segurança deve levar em conta o panorama complexo da informação em saúde, devendo, portanto, ser robusta e flexível o suficiente para se ajustar aos aspectos ético-legais na área da saúde e aos diversos tipos de informação e usuários existentes".

E, ainda segundo os autores,

> "Deve prover, em caso de necessidade, apresentar soluções específicas para atender a determinados aspectos pertinentes a algum tipo de dado, como por exemplo, a questão da integridade e autenticidade das imagens médicas, tendo como meta primária a manutenção da segurança da privacidade e da confidencialidade dos dados do paciente, sem prejudicar o atendimento e a pesquisa".

Observa-se, segundo Smith e Eloff [38], que existe um paradoxo inerente aos registros em saúde, que a segurança necessita atender: "proteger totalmente os dados do paciente, dada a sua natureza extremamente sensível, ao mesmo tempo em que se deve disseminá-los ao máximo para prover e desenvolver diagnósticos, tratamentos e pesquisas consistentes".

Cumpre, também, lembrar aqui que as pessoas precisam ter a confiança e a segurança de que os sistemas em saúde irão salvaguardar suas informações pessoais em saúde, assegurando a relação estabelecida entre médico-paciente: "a obrigação de sigilo por parte do profissional e o direito do paciente em manter privadas as informações reveladas, conferem uma dupla natureza à confidencialidade, transformando-a em um direito-dever" [39].

Esta obrigação remonta à Antigüidade com o juramento de Hipócrates [40], base do conceito do consentimento esclarecido, que queremos também estabelecer com o intuito de

garantir a autonomia do paciente na decisão de utilização e divulgação de suas informações, sabendo-se que exceções à regra deste consentimento são necessárias, como para certas divulgações úteis para a saúde pública, ações de vigilâncias em saúde ou em situações de emergências.

2.3.1 Ética Médica.

A base teórica para a discussão da ética nesta dissertação é o livro "Princípios de ética biomédica", de Tom L. Beauchamp e James F. Childress [41]. Nesse livro, o Prof. Dr. Léo Pessini, escreveu a introdução à edição brasileira da obra, na qual consta que "qualquer tentativa de entendimento da história da bioética passa obrigatoriamente por esta obra, que inaugurou um novo paradigma de pensar as questões éticas no campo da saúde e da medicina nos EUA, o chamado principialismo" (p.9) [41].

Bioética: esta denominação é atribuída ao oncologista norte-americano Van Rensselaer Potter [42], que a utilizou pela primeira vez no livro *Bioethics: bridge to the future*. Seu objetivo era promover um novo diálogo entre ciência e humanismo que antes pareciam incapazes de comunicar-se.

Na origem da reflexão ética principialista norte-americana está a preocupação pública com o controle social da pesquisa em seres humanos e a reação a partir de três casos notáveis.

> (1) em 1963, no Hospital Israelita de doenças crônicas de Nova York, foram injetadas células cancerosas vivas em idosos doentes;
> (2) entre 1950 e 1970, no hospital estatal de Willowbrook (NY), injetaram hepatite viral em crianças retardadas mentais;
> (3) desde os anos 1940, mas descoberto apenas em 1972, no caso de *Tuskegge study* no estado do Alabama, foram deixados sem tratamento 400 negros sifilíticos para pesquisar a historia natural da doença. A pesquisa continuou até 1972, apesar da descoberta da penicilina em 1945 (p.9-10) [41].

Em reação a esses escândalos, e através da criação, via congresso americano, da *National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research* (Comissão Nacional para Proteção dos Temas Humanos da Pesquisa Biomédica e Comportamental), foi publicado, em 1978, o *Report Belmont* (Relatório de Belmont).

> Após quatro anos de trabalho, a Comissão propôs um método complementar, baseado na aceitação de que "três princípios éticos mais globais deveriam prover as bases sobre as quais formular, criticar e interpretar algumas regras específicas". A comissão reconhecia que outros princípios poderiam também ser relevantes, porém três foram identificados como fundamentais (p.10) [41].
> Os três princípios identificados pelo Relatório de Belmont foram: o respeito pelas pessoas (autonomia), a beneficência e a justiça.
> O Relatório Belmont, documento brevíssimo por sinal, inaugurou um novo estilo ético de abordagem metodológica dos problemas envolvidos na pesquisa com seres humanos. A partir daí, as questões éticas não são mais analisadas a partir dos códigos juramentos, mas a partir desses três princípios com os procedimentos práticos deles conseqüentes (p.11) [41].

Beauchamp e Childress oferecem uma análise sistemática dos princípios morais que devem ser aplicados à biomedicina e para a área clínico-assistencial, sugerindo quatro deles como base de uma teoria bioética consistente: Autonomia, Beneficência, Não maleficência e Justiça. Uma Ética que estuda a vida, tanto na sua origem, como no seu desenvolvimento e no seu fim, justificando determinadas práticas e posições baseadas em argumentos fundamentados em alguma teoria.

Códigos de ética profissional (Moralidade e teoria ética)

Segundo os autores, "os desenvolvimentos científicos, tecnológicos e sociais ocorridos durante esse período produziram mudanças rápidas nas ciências biológicas e nos cuidados com a saúde. Esses desenvolvimentos desafiaram muitas das concepções prevalecentes acerca das obrigações morais dos profissionais da saúde" (p.17) [41].

> "... os profissionais podem erroneamente supor que, seguindo obedientemente as regras do código, cumprem todas as exigências morais, assim como muitas pessoas acreditam que se eximem de todas as suas obrigações morais ao respeitar todas as exigências legais relevantes" (p.22) [41].

O respeito à autonomia

No contexto médico os problemas de autonomia decorrem da condição dependente do paciente e da posição de autoridade do profissional.

> "... a autonomia e a autoridade são incompatíveis, mas não porque os sejam intrinsecamente incompatíveis. Os conflitos surgem porque a autoridade não foi propriamente delegada ou aceita".

> "... As regras ou códigos de ética profissional, do mesmo modo, não são invenção de um individuo, e, no entanto, são compatíveis com a autonomia" (p.142) [41].
> "... O respeito à autonomia fornece a principal base justificadora das regras de informação e de consentimento. O consentimento não pode expressar autonomia a menos que seja um consentimento informado assim ao se informar o paciente, um consentimento válido depende de uma comunicação honesta" (p.426) [41].

Os autores empregam o conceito do principio do respeito à autonomia, e sua importância, para examinar a tomada de decisão na assistência médica, fundamentados nas filosofias de Immanuel Kant [43]: "o respeito à autonomia origina-se do reconhecimento de que todas as pessoas têm valor incondicional, e de que todas têm capacidade para determinar o próprio destino", e John Stuart Mill [44], "às vezes somos obrigados a procurar persuadir os outros, quando eles têm opiniões falsas ou não-ponderadas".

> "Esse princípio necessita de especificação em contextos particulares para se tornar um guia prático para conduta, na identificação do que é protegido pelas regras do consentimento informado, recusa informada, veracidade, privacidade e confidencialidade. O principio de respeito à autonomia como suas especificações são prima facie, não absolutos" (p.144) [41].

2.3.2 O relacionamento entre o profissional de saúde e o paciente - Privacidade, Confidencialidade e o Consentimento Esclarecido.

Apresentam-se, a seguir, os principais aspectos que no enfoque desta dissertação são indispensáveis e que devem permear a relação do profissional de saúde com o paciente.

Privacidade e Confidencialidade.

No trato com as informações do paciente os profissionais de saúde se deparam com situações delicadas e, ao revelar ou não uma informação importante sobre o paciente, acabam vivenciando dilemas que são interpretados até como má conduta profissional.

Segundo Beauchamp e Childress (p.436) [41], resulta que esses profissionais, por vezes, se vêem diante de um conflito, pois ao mesmo tempo em que têm obrigação com a privacidade e a confidencialidade dessas informações, também têm compromisso com a veracidade e a fidelidade dos fatos, o que poderá implicar ou não a revelação das mesmas.

Exemplificando esse conflito entre as obrigações de privacidade e de confidencialidade, os autores citam o caso específico da AIDS e de suas políticas para controlar epidemia. Intromissões justificadas, por meio da ponderação de interesses legítimos na submissão das pessoas a exames, visando à determinação de resultados positivos para os anticorpos do HIV, representa uma ameaça de perda de privacidade. Ao mesmo tempo, os médicos questionam a obrigação de confidencialidade no momento em que tomam ciência de que os pacientes portadores do vírus da AIDS se recusam a informar ou a permitir que seus cônjuges ou parceiros sexuais sejam informados sobre sua condição.

Na verdade, não obstante serem intimamente ligados, privacidade e confidencialidade são termos distintos com conceitos também distintos, porém com parcial sobreposição. Quando o paciente não permite o acesso às suas informações é comum ouvir-se que o acesso desautorizado infringe o direito de confidencialidade e, por vezes, que infringe o direito de privacidade. Mas, no caso de outra pessoa qualquer acessar as informações do paciente, sem a permissão necessária, esta estará violando o direito de privacidade e não o direito de confidencialidade.

Isto mostra que: "uma violação do direito de confidencialidade de X só ocorre se a pessoa a quem X revelou a informação em confiança não protege a informação ou deliberadamente a revela a um terceiro sem o consentimento de X" (p.453) [41].

As definições de privacidade que têm por base o controle sobre o acesso às informações de um paciente são limitadas, uma vez que se concentram nos poderes e direitos ao invés de focar as condições de privacidade e por isso, não se constituem em elemento necessário e suficiente da privacidade. Por outro lado, defini-la em termos dos diversos tipos de acesso restrito se torna amplo demais. De acordo com os autores,

> "O direito constitucional à privacidade ainda é rudimentar e controverso, e o atual estado de lei estatutária e baseada em precedente judicial é caótico. Pode-se esperar maiores desenvolvimento legais. [...] Essas questões tornam-se ainda mais complicadas com as concepções divergentes da privacidade e com as discordâncias quanto aos fundamentos, aos limites e ao peso do direito de privaciade" (p.440) [41].

Há de se perceber, no entanto, que a flexibilidade do conceito de privacidade faz com que seja necessário o estabelecimento de uma significação mais rígida, o que acaba por ser útil às políticas.

Nesse âmbito, Beauchamp e Childress (p.441) [41], sugerem que: "os que propõem as políticas especifiquem cuidadosamente as condições em que o acesso é restrito e que constituirão perda ou violação da privacidade". E seguem esse raciocínio afirmando também que,

> "A política deve definir acuradamente as esferas que são consideradas privadas e que não devem ser invadidas, e deve também determinar os interesses que podem ser legitimamente contrapostos aos interesses de privacidade. Muitas vezes o enfoque estará sobre a privacidade de informações e as formas restritivas de acesso a informações sobre as pessoas; em outras ocasiões, porém, as políticas tratarão da privacidade nas tomadas de decisão, nos relacionamentos íntimos e assim por diante" (p.441) [41].

Ao ingressar voluntariamente em um hospital, o paciente consente explicita e implicitamente o acesso a sua pessoa, ciente de que estará sujeito a certas perdas de privacidade, porém a sua decisão de entrar no hospital não significa que concedeu acesso irrestrito a sua pessoa. Interessante observar que quando se concede acesso a outras pessoas, mesmo ciente da perda de privacidade é possível manter algum controle sobre as informações geradas, pelo menos em contextos terapêuticos, de diagnóstico e em pesquisas. Pois somente será acusada de violar os direitos de confidencialidade aquela pessoa a quem se consentiu o acesso às informações.

Vale acrescentar que as ameaças à confidencialidade também estão presentes em muitas instituições que se dedicam a armazenar e disseminar informações médicas confidenciais. "Em termos esquemáticos, a informação I é confidencial se, e somente se, A revela I a B, e B promete não revelar I a nenhum terceiro C sem o consentimento de A" (p.456) [41].

Uma informação confidencial caracteriza-se como tal quando é fornecida de maneira voluntária e privada, em uma relação pautada pela confiança. No caso de um paciente estar participando de uma pesquisa e autorizar que outros acessem suas informações, não se considera que tenha havido violação de direitos de confidencialidade, mesmo que possa existir alguma perda de confidencialidade e de privacidade.

Para tanto, é preciso que a política de confidencialidade proíba revelações de informações. Desta forma, exemplificando:

> "Serão seguidas regras estritas de confidencialidade. Dados individuais não serão relatados. Só serão comunicados os resultados agregados e sumários. A identidade dos indivíduos permanecerá oculta, e nenhuma informação será associada a eles nem afetará seu emprego ou sua utilização dos serviços de saúde. (...) Todos terão garantia de confidencialidade quanto aos dados coletados. Ademais, o acesso às informações será restrito aos principais pesquisadores" (p.456) [41].

Entretanto, algumas exceções, morais e legais, são admitidas e justificáveis ao que deve ser considerado confidencial nas políticas. Pode-se estabelecer limites a confidencialidade por meio de obrigações legais e obrigatórias, como nos casos de doenças contagiosas, abusos com crianças e ferimentos causados com arma de fogo.

O Consentimento Esclarecido

Tendo como finalidade a garantia da autonomia do paciente e a delimitação da responsabilidade do profissional de saúde, o consentimento esclarecido e expresso é o paradigma básico da autonomia na saúde, na política e em outros contextos.

De acordo com Beauchamp e Childress (p.162) [41]:

> "O enfoque se transferiu da obrigação do médico ou do pesquisador de revelar a informação para a qualidade do atendimento e do consentimento de um paciente ou de um sujeito de pesquisa. As forças por trás dessa modificação na ênfase foram impelidas pela autonomia e, também, fundamentalmente, externas aos códigos da ética médica e da ética da pesquisa".

Não se pode deixar de dizer, no entanto, que alguns debatedores tentaram reduzir a noção do consentimento esclarecido a uma decisão oriunda de um consenso obtido entre o médico e o paciente, resultando que consentimento informado e decisão conjunta se tornaram sinônimo. Este fato não significa que consentimento informado tenha esse significado na linguagem comum ou na lei, mas que deveria tê-lo. Tal idéia é aceitável quando o consentimento envolve as trocas de informações entre os pacientes e os profissionais de saúde, evidenciando mais do que apenas autorizar uma intervenção. Fato que embasa a opção desta dissertação por adotar, doravante, o termo consentimento esclarecido.

A justificação das obrigações de confidencialidade

Ciente de que se está tratando de garantias à privacidade e à confidencialidade das informações do paciente, cumpre dizer que não se possa revelar informações recebidas de outrem em um relacionamento particular. Por isso, a discussão sobre as diferentes regras de confidencialidade baseia-se parcialmente em alegações empíricas sobre qual regra seria mais eficaz para o alcance do objetivo esperado, qual seja proteger as pessoas.

De acordo com Beauchamp e Childress (p.459) [41], são três as regras para proteger a confidencialidade:

> Argumentos de base conseqüencialistas - Um médico que viola a confidencialidade também não pode ignorar o potencial de desgaste do sistema de confidencialidade, confiança e fidelidade médicos. Uma justificação conseqüencialista para a violação da confidencialidade só pode cumprir seus próprios exigentes critérios se tais conseqüências forem levadas em consideração.
> Argumentos baseados em direitos de autonomia e privacidade – A principal tese é que o valor da privacidade dá um peso considerável às regras de confidencialidade que a protegem. O reconhecimento, no direito consuetudinário, no direito estatutário e na constituição, da proteção dos interesses de privacidade apóia este argumento, mas trata-se antes de uma tese moral que de uma tese legal.
> Argumentos baseados na fidelidade – O contexto de prática médica requer a revelação de informações particulares e delicadas, e, portanto, a falta de fidelidade fere uma dimensão significativa da relação médico-paciente. Parte da força do compromisso de confidencialidade deriva de uma promessa implícita ou explícita por parte do profissional para com a pessoa que busca ajuda.

Ressalta-se a necessidade de compreender as condições em que as obrigações de confidencialidade podem ser licitamente superadas por obrigações preponderantes, o que denota que nenhum dos três argumentos se consubstancia em regras absolutas de confidencialidade. Em outras palavras: “Qualquer que seja sua base, estas regras são prima facie, e não absolutas – tanto na ética como na lei” (p.460) [41].

Tais obrigações de confidencialidade médica não estão bem delineadas, necessitando de reestruturação. Se, de um lado honram-se as obrigações de respeito à autonomia, os pacientes devem ser informados sobre as práticas de confidencialidade e das ameaças que podem sofrer, assim como bancos de dados informatizados. Os pacientes deveriam poder consentir a inclusão de informações em seus registros e ter acesso a esses registros, além de um controle sobre o acesso que outros possam ter a esses registros.

Desta forma, Beauchamp e Childress (p.451-2) [41] concluem,

> ... devemos ressaltar que diversas concepções da ética do caráter exibem um padrão de convergência similar e que os apelos aos princípios são muitas vezes intercalados com apelos às virtudes. Aristóteles e Hume, por exemplo, com freqüência concordam ao recorrer às virtudes e em suas concepções sobre elas, e, embora os dois sejam fundamentalmente teóricos das virtudes, ambos reconhecem a importância dos princípios normativos gerais. Também Kant e Mill exibem uma profunda preocupação com aquilo que Mill chama de "o cultivo geral da nobreza de caráter". Quase todas as grandes teorias convergem para a conclusão de que o mais importante elemento da vida moral de uma pessoa é um caráter desenvolvido que proporcione a motivação e a força interiores para fazer o que é certo e bom.

2.3.3 Código de ética médica

Na resolução do CFM, nº 1931/2009 [22], que aprova o Código de Ética Médica, em seu Capítulo IX (SIGILO PROFISSIONAL), consta que:

> É vedado ao médico:
> Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.
> Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha. Nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento; c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal.
> Art. 74. Revelar sigilo profissional relacionado a paciente menor de idade, inclusive a seus pais ou representantes legais, desde que o menor tenha capacidade de discernimento, salvo quando a não revelação possa acarretar dano ao paciente.
> Art. 75. Fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos, em meios de comunicação em geral, mesmo com autorização do paciente.
> Art. 76. Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.
> Art. 77. Prestar informações a empresas seguradoras sobre as circunstâncias da morte do paciente sob seus cuidados, além das contidas na declaração de óbito, salvo por expresso consentimento do seu representante legal.
> Art. 78. Deixar de orientar seus auxiliares e alunos a respeitar o sigilo profissional e zelar para que seja por eles mantido.
> Art. 79. Deixar de guardar o sigilo profissional na cobrança de honorários por meio judicial ou extrajudicial.

A importância dos mecanismos estabelecidos pelas leis, resoluções e códigos de comportamento na intermediação das relações sociais, segundo Neves (p.39) [45], garante a convivência harmônica e respeito mútuo dos cidadãos. "Não basta o ser humano conhecer o que é certo e errado para escolher o certo, é necessário haver limites legais e punições para a regulamentação profissional". Esta afirmação ganha ainda mais força quando se trata de uma atividade como a atenção à saúde que permite a um ser humano, o profissional de saúde, invadir o corpo e mente de outro ser humano, o paciente. "Nestas circunstâncias nada é absoluto, porque se trata da pessoa humana. Trata-se de gente, gente que cuida de gente. Gente que precisa de limites para respeitar seu semelhante" (p.39) [45].

Por exemplo, o código de Ética Médica se aplica sobre um conjunto de normas ligadas ao procedimento do médico durante o chamado ato médico, ou seja, em plena atividade profissional. Ele tem um enfoque educativo e outro punitivo, a estrutura destes códigos é disposta em capítulos e estes se dividem em artigos, abordando diversos temas relativos ao relacionamento dos médicos com seu meio. Todas estas iniciativas foram legitimadas por conselhos ou ordens que integram as diferentes profissões de saúde do país, e posteriormente foram promulgadas pelos governos federais, tornando-se lei para a classe.

Os códigos de Ética Médica brasileiros tiveram sua origem histórica e a evolução dos seus princípios a partir da tradição hipocrática até o desenvolvimento técnico-científico atual. Com a criação do Conselho Federal de Medicina, em 13 de setembro de 1945, através do Decreto-Lei nº 7955 [7], e adquirindo suas características atuais a partir de 30 de setembro de 1957, pela Lei nº 3268 [7], ocorreu o aprimoramento destes códigos.

De acordo com Neves (p.45) [45], "Os princípios do código de Ética Médica não são leis imutáveis, destinadas a controlar o médico, mas sim, um norte ao qual ele deve guiar sua conduta. Aos Conselhos Federal e Regionais de Medicina, cabe interpretar esses princípios de acordo com cada circunstância".

2.3.4 Código de ética dos profissionais de informática em saúde

Segundo a International Medical Informatics Association (IMIA),

> "O Código de Ética para Profissionais de Informática em Saúde, deve ser flexível o suficiente para se adaptar a mudanças sem, no entanto, sacrificar a aplicabilidade de seus princípios básicos. Torna-se, portanto inapropriado que este Código enfoque as especificidades de todas as possíveis situações que possam surgir. Isto poderia tornar este Código pouco adaptável, muito rígido, e muito dependente do estado corrente da Informática. Ao invés disto, tal Código deve privilegiar a abordagem de questões éticas do especialista em Informática em Saúde, e as relações entre estes profissionais e os interlocutores com os quais interagem profissionalmente. Estes grupos de interlocutores incluem (embora não se limitem a) pacientes, profissionais da Saúde, pessoal administrativo, instituições de Saúde, bem como operadoras de planos de saúde, agências governamentais etc" [46].

Os profissionais de informática em saúde desempenham um papel ímpar no planejamento e prestação de serviços de saúde, diferentes daquele dos profissionais de informática que trabalham em outras áreas, como por exemplo, ao influenciarem na operacionalização do Prontuário Eletrônico do Paciente (PEP). Este aglutina informações confidenciais obtidas na relação paciente-profissionais de saúde, justificando, dessa maneira, a razão que orientou a elaboração de um Código de Ética para Profissionais de Informática em Saúde, ao invés de simplesmente adotar algum dos outros códigos existentes para as várias associações de profissionais de informática.

> "Os Profissionais de Informática em Saúde se tornam parte integrante de uma teia de relacionamentos sujeitos a restrições éticas especiais. Portanto, acima destas restrições éticas que surgem da relação entre o PEP e o próprio paciente, a conduta ética dos Profissionais de Informática em Saúde também está sujeita às considerações que emergem das interações entre eles e outros profissionais de saúde, instituições de saúde e outras agências. Estas restrições atuam em diferentes direções. Torna-se, portanto, imperativo que os Profissionais aos quais este Código se destina tenham idéias claras de como resolver estes conflitos de forma apropriada. Neste sentido, este Código de Ética se constitui numa ferramenta que pode ser usada em casos de colisão entre papéis e restrições conflitantes" [46].

A conduta ética ultrapassa os requisitos legais. Incontestavelmente são as leis que regulam as atividades dos profissionais de informática em saúde, embora a flexibilidade das diretrizes exigidas por uma área em constantes mudanças tecnológicas define um perfil diferenciado para os profissionais de informática em saúde. "Profissionais de Informática

em Saúde que se limitassem a seguir a lei, e que guiassem suas condutas apenas pelos precedentes legais, estariam mal preparados para lidar com situações não previstas pelos legisladores e sujeitar-se-iam às incertezas de processos judiciais futuros" [46].

Fundamentado nos princípios éticos básicos, aplicáveis aos diferentes tipos de situações que caracterizam as atividades do profissional de informática em saúde e centrado na definição das ocupações dessa profissão, o código de ética dos profissionais de informática em saúde independe dos rumos de processos judiciais e, mais do que proceder segundo a lei pode muito bem orientá-la.

> "Ao invés de se tornar ultrapassado pelas mudanças tecnológicas ou modelos administrativos, pode perfeitamente indicar as direções que estes desenvolvimentos devam seguir. Desta forma, embora em muitos casos as cláusulas deste Código venham a refletir injunções jurídicas ou normas administrativas, ele irá prover diretrizes em casos de incerteza legal ou administrativa ou em locais onde as leis e normas administrativas correspondentes não existam. Num âmbito mais geral, este Código pode até mesmo ajudar a resolver problemas apresentados pelos imperativos tecnológicos. Nem tudo que pode ser feito deve ser feito. Um Código de Ética auxilia na definição do panorama ético" [46].

3. Materiais e Métodos.

3.1 Metodologia.

A metodologia adotada para esta dissertação consistiu de um levantamento bibliográfico nas principais bases de informação científica (bases bibliográficas referencias e de texto completo) da área de Saúde, da Ciência da Informação e da Ciência da Computação de forma a identificar as diversas abordagens conceituais com que a privacidade, confidencialidade e o consentimento esclarecido vêm sendo tratados nessas áreas.

Este embasamento teórico subsidiou a análise crítica com o objetivo de conceituar privacidade, confidencialidade e o consentimento esclarecido, determinando suas aplicabilidades e quais as exceções e em quais circunstâncias se justificaria a revelação, não autorizada, das informações confiadas nesta relação especial entre médico e paciente, nos sistemas de informações sob a responsabilidade do DATASUS, mais especificamente no Prontuário Eletrônico de Paciente (PEP), do Sistema de Gerenciamento de Informações Locais (GIL).

Este levantamento bibliográfico teve o ano de 1998 como limite inferior para o escopo temporal, ou seja, foi realizado a partir de 1998, período de introdução das tecnologias para a segurança das informações de forma mais intensiva na gestão das informações em saúde.

As etapas de desenvolvimento da dissertação foram:

1. Busca bibliográfica consistente na literatura existente cujos temas estejam relacionados com segurança da informação e segurança das informações em saúde, com ênfase na confidencialidade, privacidade e no consentimento esclarecido das informações médicas dos pacientes;
2. Análise sistemática de conceitos e de propostas (alternativas) para a privacidade, a confidencialidade e o consentimento esclarecido evidenciando suas aplicações operacionais nos Registros Eletrônicos em Saúde (RES);
3. Análise da aplicação dos conceitos de confidencialidade, privacidade e o consentimento esclarecido na segurança das informações do PEP / GIL;

4. Análise do nível de segurança para a interoperabilidade do PEP / GIL;
5. Propostas para identificar os mecanismos que poderiam ser implementados nos registros de diagnósticos do PEP / GIL, visando sempre garantir a confidencialidade e privacidade da relação médico-paciente, comparando como o Plano Diretor de Segurança da Informação (PDSI) trata a segurança da informação dos Sistemas de Informações em Saúde (SIS) sob responsabilidade do DATASUS.

A análise do material investigado teve sempre como foco, a identificação da relevância da privacidade e da confidencialidade e do consentimento esclarecido, e de mecanismos que os resguardem, assim como de suas características, no contexto das relações entre profissionais de saúde e pacientes, que possam ser aplicáveis aos SIS do DATASUS, mais especificamente ao PEP / GIL.

3.2 Estruturas e definições do DeCS para os Termos do Levantamento Bibliográfico.

Após a escolha das palavras-chave:

a) Sistemas de Informação em Saúde;
b) Confidencialidade;
c) Privacidade;
d) Consentimento Esclarecido;
e) Prontuário do Paciente;
f) Segurança da Informação;
g) Responsabilidade pela informação.

Foi realizado o levantamento dos termos adotados para o levantamento bibliográfico e suas equivalências no *tesaurus* reconhecido da área de saúde, o DeCS – Descritores em Ciências da Saúde, nesta etapa foram encontrados os seguintes resultados:

Sistemas de Informação

Descritor Inglês: ***Information Systems***.
Descritor Espanhol: ***Sistemas de Información***.
Descritor Português: **Sistemas de Informação**.
Sinônimos em Português: Sistemas de Dados, Sistemas de Apoio a Informação, Sistemas de Informação de Atendimento de Emergência e Sistemas de Recuperação de Informação.

Definição em Português: Grupo integrado de arquivos, procedimentos e equipamentos para o armazenamento, manipulação e recuperação de informações.

Nota de Indexação em Português: para sistemas automatizados não coordenados com PROCESSAMENTO AUTOMATIZADO DE DADOS; para sistemas de informação médica não coordenados com MEDICINA.

Confidencialidade (Comunicação sigilosa)

Descritor Inglês: ***Confidentiality***.
Descritor Espanhol: ***Confidencialidad***.
Descritor Português: **Comunicação Sigilosa**.
Sinônimos em Português: Privacidade dos Dados do Paciente e Comunicação Privilegiada.

Definição em Português: Privacidade de informação e proteção contra revelação não autorizada.

Nota de Indexação em Português: segredo é indexado aqui.

Descritores Relacionados em Português: Testes Anônimos, Revelação, Responsabilidade pela Informação, Privacidade Genética, Notificação aos Pais e Privacidade.

Privacidade

Descritor Inglês: ***Privacy***.
Descritor Espanhol: ***Privacidad***.
Descritor Português: **Privacidade**.
Sinônimos em Português: Direito a Privacidade, Direito de Propriedade, Direito Individual, Direito Pessoal, Direito Privado e Lei Pública 93-579 (EUA).

Definição em Português: O estado de estar livre de intrusão ou perturbação na vida privada de uma pessoa ou em seus negócios.

Nota de Indexação em Português: um direito civil à liberdade contra intrusão em assuntos privados; um estatuto Federal; privacidade de dados ou registros de pacientes: indexe sob COMUNICAÇÃO SIGILOSA.

Descritores Relacionados em Português: Comunicação Sigilosa, Espaço Pessoal e Auto-Revelação.

Consentimento Esclarecido

Descritor Inglês: ***Informed Consent***.
Descritor Espanhol: ***Consentimiento Informado***.
Descritor Português: **Consentimento Esclarecido**.
Sinônimos em Português: Autorização Consciente, Consentimento Consciente e Consentimento esclarecido.

Definição em Português: Autorização voluntária dada por um paciente ou sujeito da pesquisa, com total compreensão dos riscos envolvidos nos procedimentos de diagnóstico ou de pesquisa e para tratamento médico ou cirúrgico.

Nota de Indexação em *Português*: competência em consentir: coord como primário com COMPETÊNCIA MENTAL (como primário).

Descritores Relacionados em *Português*: Revelação, Competência Mental e Recusa do Paciente ao Tratamento.

Prontuário do Paciente

Descritor Inglês: ***Medical Records Systems, Computerized***.
Descritor Espanhol: ***Sistemas de Historias Clínicas Informatizadas***.
Descritor Português: **Sistemas Computadorizados de Registros Médicos**.
Sinônimos em Português: Sistemas Automatizados de Registros Médicos, Prontuário Eletrônico e Registros Computadorizados de Pacientes.

Definição em Português:
Sistemas baseados em computadores para admissão, estoque, demonstração, recuperação e impressão de informação contida em um registro médico do paciente.

Nota de Indexação em *Inglês*: DF: *AUTOMATED MED RECORDS*.

Segurança da Informação

Descritor Inglês: ***Computer Security***.
Descritor Espanhol: ***Seguridad Computacional***.
Descritor Português: **Segurança (computação)**.
Sinônimos em Português: Vírus de Computador, Proteção de Dados e Segurança de Dados.

Definição em Português: Medida de proteção contra acesso sem autorização ou interferência com sistemas operacionais de computador, telecomunicações ou estruturas de dados, especialmente a modificação, apagamento, destruição ou liberação de dados em

computadores. Inclui métodos de evitar interferência por vírus de computador ou os denominados *hackers* de computador que almejam comprometer dados armazenados.

Nota de Indexação em Português: contra acesso sem autorização a computadores & bases de dados: veja definição; não use para confidencialidade de registros (= COMUNICAÇÃO SIGILOSA + REGISTROS COMO ASSUNTO ou termo de registro específico).

Responsabilidade pela informação

Descritor Inglês: ***Duty to Warn***.
Descritor Espanhol: ***Deber de Advertência***.
Descritor Português: **Responsabilidade pela Informação**.
Sinônimos em Português: Dever de Avisar, Dever de Informar e Dever de Prevenir.

Definição em Português: Obrigação do profissional da saúde de quebrar a CONFIDENCIALIDADE do paciente para notificar terceiros sobre o risco de ser acometido ou de contrair infecção grave.

Descritores Relacionados em Português: Comunicação Sigilosa, Dever de Recontatar e Notificação de Abuso.

4. O Levantamento Bibliográfico

O levantamento teórico inicial para os termos escolhido (09/2009) foi realizado nas duas principais bases de informação científica (bases bibliográficas referencias e de texto completo) das áreas da Saúde, da Ciência da Informação e da Ciência da Computação: a Medical Literature Analysis and Retrieval System Online (MEDLINE) e a Literatura Latino-Americana e do Caribe em Ciências da Saúde (LILACS).

Base de dados: **MEDLINE_1997-2009**

Pesquisa: **[Descritor de assunto]**	Referências encontradas
sistemas de informação	**4832**
confidencialidade (comunicação sigilosa)	**8700**
privacidade	**2370**
consentimento esclarecido	**13246**
sistemas computadorizados de registros medicos	**11978**
segurança (computação) - L01.209 [Categoria DeCS]	**697**
responsabilidade pela Informação	**495**
Total	**42318**

Base de dados: **LILACS**

Pesquisa: **[Descritor de assunto]**	Referências encontradas
sistemas de informação	**1533**
confidencialidade (comunicação sigilosa)	**150**
privacidade	**35**
consentimento esclarecido	**438**
sistemas computadorizados de registros medicos	**98**
segurança (computação) - L01.209 [Categoria DeCS]	**10**
responsabilidade pela Informação	**27**
Total	**2291**

A pesquisa isolada dos termos, nas bases de dados MEDLINE (1997 / 2009) e LILACS, levaram a um número (42318 + 2291 = 44600) inviável para o levantamento proposto. Analisando aleatoriamente alguns resumos desta pesquisa sentiu-se a necessidade do cruzamento dos termos, buscando a aproximação das referências encontradas com objetivo deste levantamento.

A indexação pelos descritores confidencialidade e privacidade, considerados praticamente sinônimos para o DeCS, tornou o resultado do levantamento para o termo privacidade, praticamente, um subconjunto da seleção para o termo confidencialidade (comunicação sigilosa) e/ou vice-versa, evidenciando na maioria dos textos, um enfoque (privacidade = confidencialidade) conflitante com o do objeto, dificultando a seleção dos textos básicos para o embasamento teórico necessário para atingir os resultados propostos por esse levantamento bibliográfico.

Outra questão suscitada foi, qual seria o termo principal e mais adequado para o levantamento bibliográfico: Segurança da Informação, Sistemas de Informação ou Prontuário Eletrônico (sistemas computadorizados de registros médicos)? A opção foi por

Sistemas de Informação (SI), pois tanto os aspectos da confidencialidade, quanto os da privacidade, na especificidade das pesquisas, nortearam o rumo da segurança da informação (ver nota de indexação Português, na definição do termo em estrutura do DeCS), e por ser mais abrangente para informação em saúde, do que sistemas computadorizados de registros médicos, termo definido para prontuários eletrônicos. A escolha por SI foi uma tentativa de enriquecer a discussão entre Registros Eletrônicos em Saúde (RES) e Prontuário Eletrônico do Paciente (PEP), proposta por esta dissertação.

Levantamento para **sistemas de informação** como termo principal em cruzamento com:

Base de dados: **MEDLINE_1997-2009**

Pesquisa: **[Descritor de assunto]**	Referências encontradas
confidencialidade (comunicação sigilosa)	**182**
privacidade	**34**
consentimento esclarecido	**10**
responsabilidade pela informação	**0**
Total	**226**

Nota: O fato de o resultado da pesquisa pelo cruzamento dos termos **sistemas de informação** e **responsabilidade pela informação** não apresentar nenhum texto, indica a independência dos termos, isto é, a responsabilidade pela informação e a confidencialidade das informações do profissional de saúde, é desvinculada da responsabilidade do armazenamento e da disseminação nos Sistemas de Informações em Saúde (SIS).

Base de dados: **LILACS**

Pesquisa: **[Descritor de assunto]**	Referências encontradas
confidencialidade (comunicação sigilosa)	**1**
privacidade	**0**
consentimento esclarecido	**1**
responsabilidade pela informação	**0**
Total	**2**

Seleção dos textos da pesquisa

Dos textos encontrados com o cruzamento de **sistemas de informação** com o termo **confidencialidade (comunicação sigilosa),** na Base de dados **MEDLINE_1997-2009**, selecionou-se pelo título e pelo resumo 40 referências. Após esta análise inicial, os textos que apresentaram a sua fonte em formato eletrônico, foram analisados na busca de subsídios para o presente estudo da dissertação.

Na Base de dados **LILACS** o cruzamento tendo como principal descritor **sistemas de informação** não foi um bom procedimento, apresentando como resultado textos já selecionados na Base de dados **MEDLINE_1997-2009,** tanto para o cruzamento com **confidencialidade** (**comunicação sigilosa**), quanto para **consentimento esclarecido**. Então buscamos os outros cruzamentos, que com exceção do cruzamento **sistemas computadorizados de registros médicos** com **confidencialidade (comunicação sigilosa),** que apresentou cinco textos, sendo 1(um) selecionado, não apresentaram textos aproveitáveis.

Alguns textos não apresentam a forma eletrônica para consulta, e só podem ser acessados através de fotocópias. Caso houvesse a necessidade, imprescindível, desse material para as conclusões dessa dissertação, tentar-se-ia sua disponibilização através da biblioteca da Escola Nacional de Saúde Pública (ENSP).

5. Resultados e Discussão

Os relacionamentos entre os termos propostos nortearam a forma de pesquisa para o levantamento nas duas principais bases de dados da informação científica para área da saúde, MEDLINE e LILACS. Com o foco na confidencialidade e na privacidade da segurança das informações em saúde, buscou-se estabelecer um conjunto de textos, interdependentes, que pudessem traduzir o entrelaçamento conceitual entre Sistemas de Informações em Saúde e Segurança da Informação.

A análise do resultado do levantamento e a leitura dos textos selecionados tornaram-se um exercício recursivo de ajustes e de escolhas, sempre tendo por objetivo a melhor interpretação e o melhor aproveitamento das recomendações e dos conceitos propostos pelos autores. A cronologia para a apresentação dos textos obedece à ordem decrescente da data de sua publicação.

Apresentação dos textos

Os conteúdos a seguir foram elaborados com base na leitura dos textos originais em inglês, e apresentados a partir de suas traduções livres.

01) Conn J. Critics assail HHS initiative. Framework described as lacking privacy protections. Modern Healthcare. USA. 2008 Dec.

Neste texto, de dezembro de 2008, o autor descreve críticas para as novas iniciativas de segurança e privacidade dos pacientes, do Departamento de Saúde e Serviços Humanos (*Health and Human Service - HHS*) que é a principal agência de proteção da saúde dos americanos.

Alguns especialistas em privacidade atacaram o modelo descrito, pela entidade, classificando de ineficiente e deficiente para a proteção da privacidade, afirmando que o modelo não possui detalhes que melhorariam a proteção da privacidade dos pacientes. O modelo apresenta documentos da nova política de privacidade abrangendo fornecedores e

outras organizações que lidam com informações pessoais em saúde, dos pacientes. Um documento é uma proposta para a política de privacidade, modelo a ser usado por fornecedores de registros pessoais em saúde, o outro documento é um *framework* muito mais amplo de privacidade para ajudar a guiar o desenvolvimento da rede nacional de informação em saúde (*Nationwide Health Information Network - NHIN*).

Para Pam Dixon, diretor-executivo de um Fórum Mundial de Privacidade, sem fins lucrativos, em Washington: Perdeu-se uma significativa oportunidade para acrescentar algumas inovações ao pensamento da privacidade.

Gellman Robert, um advogado e consultor de privacidade em Washington, disse que o modelo, embora bem-vindo, é de tão alto nível que não resolve nenhum dos complexos conflitos, que a política de privacidade levantará para a Troca de Informações em Saúde (TIS) entre organizações nacionais: Em outras palavras, HHS tem trabalhado fortemente (e) reinventou a roda.

O modelo, segundo o HHS, é uma ajuda inicial para que todas as partes trabalhem em conjunto, visando integrar a tecnologia de informação em saúde e as questões de privacidade. Uma resposta aos relatórios publicados desde o inicio de 2007, pelo Escritório de Responsabilidade do Governo (*Government Accountability Office*), criticando o HHS pela falta de um plano abrangente de Tecnologia da Informação (TI), para a privacidade.

Estamos tentando criar um conjunto comum de perspectivas para as pessoas que desenvolvem programas de privacidade e segurança, disse Jodi Daniel, diretor do escritório de política e pesquisa no ONCHIT (Office of the National Coordinator for Health Information Technology - ONCHIT).

As doze páginas do Modelo de Privacidade e Segurança Nacional para Intercâmbio Eletrônico de Informações em Saúde Individualmente Identificáveis tiveram por objetivo levantar questões que possam servir como possíveis opções, ou para o próximo Congresso, ou para a próxima administração.

O modelo corretamente reconhece que os indivíduos que não confiam no sistema de dados *on-line* não compartilharão suas informações. Faz recomendações a respeito da questão do controle individual sobre o compartilhamento de suas informações em saúde. Ressalta que a capacidade de indivíduos em fazer escolhas com relação à troca eletrônica de informações em saúde individualmente identificável sobre eles é importante para ganhar

confiança. De acordo com o *framework*, os participantes no ato da troca de informação em saúde, tais como organizações regionais de informações em saúde e empresas de dados, deverão proporcionar oportunidades razoáveis e capacidades para os indivíduos exercerem as suas escolhas em relação às suas informações em saúde individualmente identificáveis.

Para a Rede Nacional de Informação em Saúde (NHIN), a importância da proteção da privacidade para obter a confiança dos doentes é a chave para o sucesso. Encontrar o equilíbrio entre o aumento do acesso à informação e à privacidade é muito importante e os cidadãos não devem ser forçados a aceitar riscos para a privacidade que eles não querem.

02) Myers J; Frieden TR; Bherwani KM; Henning KJ. Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. American journal of public healt. USA. 2008 May.

As preocupações com a privacidade e a confidencialidade são ainda mais sensíveis na era digital. A troca da tecnologia de armazenamento (de papel para formato eletrônico) proporciona violações de alto-nível aos dados pessoais dos pacientes. Nesse texto os autores demonstraram suas preocupações com a confidencialidade da Saúde Pública Americana na era digital, ressaltando que a crescente necessidade das Agências Públicas de Saúde em armazenar e manter informações pessoais em saúde em formatos eletrônicos (melhora o desempenho das funções essenciais da saúde pública), e os planos de criação de redes de informações eletrônicas em saúde interconectadas, aumentaram a ansiedade sobre a privacidade das informações.

Afirmam os autores: vamos identificar e fornecer os meios para enfrentar as ameaças ao delicado equilíbrio entre a necessidade de aquisição de dados das agências de saúde pública e exigência de segurança de informações confidenciais.

Para eles, esta revisão é particularmente relevante para aqueles que estão implementando programas, mas ainda não estão completamente familiarizados com os princípios e práticas das tecnologias de segurança da informação. Uma compreensão básica destes temas é importante para a efetiva colaboração e cooperação com colegas em vários campos, incluindo os da tecnologia da informação.

Pregavam, a efetiva colaboração e cooperação dos profissionais públicos de saúde com os profissionais da tecnologia da informação. Segundo os autores, políticas preventivas, como, medidas práticas e educacionais, engenharias (mecanismos) para controles de acesso e algumas tecnologias emergentes, podem ser implementadas para proteção e fortalecimento da segurança dos dados. O fracasso das ações preventivas pode pôr tanto a privacidade e confidencialidade das informações individuais do paciente, como a saúde pública, em risco.

Os autores concluem que as agências de saúde pública são desafiadas a equilibrar melhor, os interesses da saúde pública com os direitos e privilégios individuais. Para isso, devem avaliar todas as ameaças e utilizar, tanto quanto possível, políticas, educação, engenharia de prevenção e as tecnologias emergentes, que possam ajudar a abordá-las, aumentando a segurança e privacidade de dados na transmissão (compartilhamento) e armazenamento (gravação/processamento).

Embora a garantia da privacidade perfeita das informações pessoais em saúde seja impossível, minimizar os riscos melhorando as competências do pessoal e a maneira como os dados são adquiridos, usados, mantidos, armazenado e compartilhado, propicia indivíduos mais suscetíveis a fornecer informações pessoais em saúde, já que possuem confiança na segurança de suas informações. As agências de saúde pública devem impor a segurança pró-ativa aos dados, pois elas dependem dos dados que recebem para promover e proteger a saúde pública.

03) Wiljer D; Urowitz S; Apatu E; DeLenardo C; Eysenbach G; Harth T; Pai H; Leonard KJ; Canadian Committee for Patient Accessible Health Record. Patient accessible electronic health records: exploring recommendations for successful implementation strategies. USA. Journal of medical internet research. 2008.

Neste texto, os autores relatam as etapas de um *Wokshop*, realizada em Toronto, Canadá, em Outubro de 2006, em resposta à necessidade de recomendações em torno da implementação do Registro Eletrônico em Saúde Acessível ao Paciente (*Patient Accessible Electronic Health Record - PAEHR*). O *Workshop* contou com 45 participantes, renomados especialistas dos Estados Unidos, Canadá, Espanha, Islândia e Holanda, para analisar

questões relacionadas com o acesso do paciente aos Registros Eletrônicos em Saúde (*Electronic Health Records - EHRs*) e com as mudanças nas gestões institucionais.

Quatro grandes domínios de assuntos foram identificados: (1) Acesso do paciente ao EHR, (2) Manutenção da privacidade e confidencialidade relacionadas com o PAEHR, (3) Educação do paciente e a navegação do PAEHR, e (4) Estratégias para mudança na gestão institucional. Foram elaboradas instruções contendo um resumo geral, uma lista de tópicos de interesse, uma lista de referência e recomendações de projetos para cada domínio de assuntos.

As discussões para o domínio dos assuntos manutenção da privacidade e confidencialidade relacionadas com o PAEHR, resumidas pela equipe de pesquisa e validadas pelos próprios participantes, foram as seguintes:

- Houve concordância entre os participantes quanto à necessidade de se adotar e manter um padrão em relação à propriedade e/ou custódia do EHR e seu conteúdo. Tradicionalmente, o prontuário do paciente tem existido sob o controle do provedor ou aos cuidados de instituição/organização. O acesso dos doentes continua aumentando, resultando em uma mudança de cultura relacionada ao controle de informações em saúde.
- Foi identificada a necessidade de criação de mecanismos locais para ajudar a gerir os conflitos potenciais resultantes de territorialismo e proteger os provedores de informações em saúde contra os riscos do compartilhamento da posse das informações com seus clientes. Em curto prazo, os provedores poderão ficar relutantes em abandonar o que tradicionalmente tem existido sob seu domínio.
- O acesso regular e permanente, por pacientes ao EHR, exige o desenvolvimento de políticas e procedimentos relacionados à gestão do registro. Os prontuários deverão ser auditados periodicamente para assegurar a exatidão, integridade e qualidade no desempenho, especialmente em situações em que as entradas do paciente são permitidas e incorporadas ao registro.
- As políticas relativas à guarda da informação têm de estar em vigor. O surgimento de portais de paciente e a capacidade de personalizar as visões do paciente podem resultar em um conjunto único de desafios. Além disso, existem

demonstrações claras de que as bases de dados institucionais dos EHR terminaram, e o início do portal do paciente precisou ser articulado.

De acordo com o texto, com base nas discussões e notas informativas para a implementação do PAEHR, no que se refere à segurança e confidencialidade, as seguintes recomendações foram definidas:

- A segurança e confidencialidade devem ser protegidas de acordo com padrões nacionais, mas ao mesmo tempo, uma mudança de paradigma (propriedade x custódia) é necessária para que as organizações de assistência médica criem uma cultura de custódia, e não da propriedade, dos dados do paciente. Essa mudança será conseguida através da criação de modelos de controle compartilhados entre profissionais de saúde, pacientes e do público em geral.
- As Organizações de saúde precisam estar confiantes de que podem controlar o risco adicional da exposição do compartilhamento eletrônico da informação do paciente com seus usuários. Os pacientes devem ter a capacidade de controlar o fluxo e de influenciar no acesso aos seus dados clínicos.

A Conclusão dos autores: O acesso aos EHRs é um direito fundamental do paciente, e os profissionais de saúde e as organizações devem mobilizar-se de forma ágil e competente para proporcionar esse acesso. Há muitas questões que precisam ser abordadas e, na falta de investigação e evidências generalizáveis, as organizações enfrentaram um quadro difícil e complexo de questões operacionais. Investigações objetivas são essenciais, e ao mesmo tempo, coordenação e esforços nacionais serão requeridos para fornecer a infra-estrutura necessária para PAEHRs. Soluções flexíveis, padronizadas e interoperáveis são necessárias para assegurar aos PAEHRs, suporte de atendimento integrado e global. Proporcionar o acesso aos EHRs, é uma etapa essencial na ativação da assistência dos pacientes e na melhoria em ampla escala do sistema de saúde.

O desafio permanece para as organizações, políticos, profissionais de saúde e cidadãos para responderem às necessidades do PAEHRs e colocarem em prática estas recomendações.

04) Boyd AD; Hosner C; Hunscher DA; Athey BD; Clauw DJ; Green LA. An 'Honest Broker' mechanism to maintain privacy for patient care and academic medical research. International Journal of Medical Informatics. Ireland .2007 May-Jun

Nesse texto, os autores apresentam um mecanismo de "Intermediação Honesto" ("*Honest Broker*") para manter a privacidade de atendimento ao paciente e a pesquisa acadêmica em saúde, visando à integração para troca de informações e dos dados em saúde entre sistemas de forma segura e confiável.

Ressaltam os autores: os médicos juraram proteger a privacidade dos pacientes. No entanto, o aumento da complexidade dos ambientes de TI, a totalização dos dados, e o desejo de outras entidades para acesso a esses dados, muitas vezes, 24 h/dia × 7 dias/semana × 365 dias/ano, estão colocando sérias dificuldades na capacidade de manter a sua segurança. Este problema atravessa todas as fontes de registro eletrônico, de registros de atendimento ao paciente e de registros acadêmicos da pesquisa médica.

Segundo o texto, existem várias iniciativas nacionais e internacionais para aumentar a conectividade dos registros eletrônicos em saúde (*Electronic Health Records - EHRs*) e para permitir a integração entre os departamentos, hospitais e outros prestadores de cuidados.

Os Institutos Nacionais de Saúde dos Estados Unidos (*US National Institutes of Health - NIH*) começavam uma pesquisa para construção de uma rede Eletrônica Nacional de Ensaios Clínicos e Pesquisa (NECTAR), permitindo que temas de investigação de diferentes centros médicos em todo o país, pudessem mais facilmente participar em grandes ensaios clínicos.

Afirmavam os autores:

- A oportunidade de proporcionar uma maior assistência ao paciente, ou de uma melhor investigação, usando os registros de dados agregados e tecnologia de rede é muito sedutora. O potencial mais emocionante deste intercâmbio de dados é que são projetos de benefício direto aos pacientes, proporcionando o conhecimento generalizável.
- O estudo de viabilidade inicial demonstrou a capacidade dos sistemas relacionados para estudar a depressão e as doenças cardiovasculares em sites

não-filiados academicamente da atenção primária, repensando a forma de armazenar, de transmitir, de processar, de acessar, e de federar (integrar a nível federal) os dados dos pacientes das aplicações clínicas e de pesquisas.

- Como parte do esforço do NIH, para a "re-engenharia da iniciativa de pesquisa clínica", estamos interligando três sistemas clínicos e um sistema de pesquisa de apoio à investigação clínica rigorosa nas não-filiadas academicamente práticas da atenção primária de uma rede regional de investigação com base na prática (*Practice-Based Research Network - PBRN*).
- Os nossos grupos da Universidade de Michigan estão desenvolvendo um sistema chamado "*Honest Broker*" para ajudar a gerenciar a comunicação entre os sistemas acima, estamos desenvolvendo um método chamado de Estrutura Clínica de Pesquisa de Informação (*Clinical Research Information Fabric - CRIF*), cujo componente central é chamado de mediador honesto (*Honest Broker - HB*).
- O *Clinfotracker* (o primário sistema de saúde), o *M-STRIDES* (o sistema de psiquiatria), o *M-CORRP* (o sistema cardiovascular) e o *Velos* (a pesquisa do sistema de coleta de dados) serão capazes de usar HB para compartilhar dados de forma segura e adequada. O HB intermedia esses sistemas, gerenciando a transferência de dados e o armazenamento eletrônico de identificadores pessoais em saúde (*electronic storage Personal Health Identifiers - ePHI*) para eles.
- Cada paciente é monitorado no *Honest Broker* através de uma identificação única atribuída internamente, que é mapeada para os correspondentes identificadores do paciente nos sistemas de participantes. Esta matriz permite o fluxo de dados de-identificados dos pacientes para o sistema de pesquisa, embora permitam essa troca de dados entre sistemas clínicos, sem tais sistemas precisarem conhecer todos os detalhes de implementação dos outros sistemas.

A partir de discussões do tipo: este projeto é pequeno em relação ao escopo das iniciativas de maior dimensão, em nível nacional e internacional, mas forneceu lições aprendidas que podem ser úteis em projetos de maior alcance. Uma lição fundamental é que combinar os registros de indivíduos entre os hospitais e clínicas, com segurança confiável, pode ser um desafio.

Concluem que embora nenhum sistema de segurança seja realmente à prova de invasão, essa arquitetura fornece um ponto de estrangulamento de alta segurança reduzindo a probabilidade de uma violação.

05) Boyd KM. Ethnicity and the ethics of data linkage. England. BioMed Central (BMC) Public Health. 2007.

Em "Etnia e a ética da articulação dos dados", o autor propôs a interligação (linkage) dos dados em saúde, com os dados do recenseamento populacional, visando a resolver a falta da informação sobre etnia nos procedimentos de rotina em saúde, registrados nos Sistemas Informatizados em Saúde (SIS), beneficiando, assim, pesquisas que envolvam, principalmente, os grupos étnicos minoritários.

Segundo o autor, um estudo na Escócia, que interligou dados em saúde e a informação de etnia de 4,6 milhões de pessoas, revelou informações importantes sobre a incidência e sobrevida após infarto agudo do miocárdio entre os sul-asiáticos. A técnica de interligação de dados, desenvolvida com a preocupação de proteger o anonimato das pessoas envolvidas (criptografia e procedimentos organizacionais, cuidadosamente elaborados para o registro da vinculação), garantiu o cumprimento da legislação de proteção de dados, recebendo aprovação reguladora apropriada.

Para Boyd KM, duas objeções éticas, conseqüência do enlace dos dados da saúde com os do recenseamento, teriam que ser respondidas: (1) a não obtenção do consentimento esclarecido; e (2) a possibilidade da informação ou desinformação pública, derivada dos resultados desses estudos, serem usadas para estigmatizar, coagir ou prejudicar fisicamente um grupo étnico minoritário.

Para a primeira objeção o autor alerta que nem todas as utilizações oficiais de informações pessoais sobre cidadãos são potencialmente inocentes e que ignorar as regras do consentimento esclarecido é moralmente perigoso. A necessidade de participação do público e a aprovação positiva terão que ser reforçadas para o exame da segunda objeção ética da vinculação de dados.

06) Dallari SG. A justiça, o direito e os bancos de dados epidemiológicos. Ciência & Saúde Coletiva. Brasil. 2007

Nesse texto a autora, como consta no resumo, constata que a compreensão das características do direito do século XXI, que enfrenta uma crise de legitimidade, e das grandes linhas que definem o relacionamento entre a sociedade e a ciência nesse século, marcado pelo risco e, conseqüentemente, pelo medo, sustentam a busca do justo equilíbrio entre a proteção individual e o desenvolvimento coletivo empreendido.

Para o direito do século XXI, a autora observa que a crise de legitimação do direito implica, portanto, a recuperação dos seus sentidos que foram sendo desprezados durante os séculos XIX e XX: o direito subjetivo, permeado pelos valores sociais, sobretudo, com a preocupação com a justiça. É necessário que, se instaure efetivamente a cidadania onde o "cidadão é aquele que tem uma parte legal na autoridade deliberativa e na autoridade judiciária", como ensina Aristóteles. E isso é especialmente verdadeiro quando se consideram as características da sociedade contemporânea, que é também chamada de "sociedade do risco".

O direito no século XXI deve refletir, então, o justo equilíbrio entre a proteção individual e o desenvolvimento coletivo, no cenário da "sociedade de risco". A situação dos bancos de dados epidemiológicos oferece um campo ideal para que se possam compreender algumas das mais importantes facetas desse equilíbrio tão precário.

Essa análise foi realizada, segundo a autora, tendo como objeto os bancos de dados epidemiológicos. Examinou-se o interesse social que pretende ter à disposição bancos de dados com as mais completas informações sobre todos os aspectos da vida das pessoas, e o interesse individual que espera o máximo respeito à esfera da vida privada de cada membro da sociedade.

Para a área da Tecnologia da Informação, a autora afirma que: do mesmo modo os sistemas deverão suportar a eventual recusa da pessoa em liberar, seja a informação a respeito dos dados clínicos, seja aquela referente às suas opções de convivência, será necessário, também, garantir que a pessoa não sofrerá qualquer prejuízo, especialmente se o banco dados for diretamente relacionado ao atendimento em saúde e caso não permita aos pesquisadores o acesso aos dados sobre ela arquivados. E será imprescindível, igualmente,

informá-la sobre as medidas para a proteção da confidencialidade do sistema e que lhe assegure a garantia da preservação do sigilo quando da publicação dos resultados da pesquisa.

Finalizando, o direito na "sociedade do risco" demanda a construção de mecanismos que permitam a decisão e o controle públicos, de todos os cidadãos, a respeito do grau de risco que pretendem correr. No caso em exame, comissões de cidadãos, peritos e populares deveriam opinar sobre a construção, a alimentação e o uso dos bancos de dados. Nesse caso, seria importante, também, tornar acessível para todos os operadores do sistema jurídico as informações relativas a tais temas do direito sanitário.

07) Kloss L. Legal implications. National standards needed to ensure interoperability, prevent fraud in Electronic Health Records (EHRs). USA. Modern Healthcare. 2005 Oct.

Nesse artigo a autora, Linda Kloss, propõe uma discussão sobre uma configuração mínima (padronização) do registro legal (de acordo com as leis) de saúde, em sua transição do formato de papel para os meios eletrônicos, necessária para assegurar a interoperabilidade e a prevenção de fraudes nos EHRs.

Para falta de uma definição acordada para o registro legal de saúde em todo os Estados Unidos, justifica com as seguintes questões: qual é a definição do registro legal médico no ambiente cada vez mais eletrônico de hoje? Quais são os conteúdos legais da transição para os registros híbridos, que são parte em papel, e parte eletrônica?.

A importância atribuída pela autora para o prontuário médico, que além de sua função essencial no atendimento clínico, é o negócio mais importante das organizações de serviços de saúde e um registro legal, fica evidente na afirmativa, independentemente do seu formato de papel, híbridos ou totalmente por via eletrônica, o registro em saúde deve satisfazer aos requisitos do registro legal e do negócio da organização. É preciso documentar e validar o processo de atendimento e seus resultados. Deve capturar indicações para o tratamento e os serviços prestados. Deve ser a base para a comunicação entre os fornecedores e para a cobrança e reembolso, julgamento jurídico, pesquisa e etc.

Ela enfatiza que as organizações de saúde estão fazendo o seu melhor, desenvolvendo políticas interna para a constituição desse registro e de sua transição para os

Registros Eletrônicos em Saúde (EHRs) e que pode ser constituído de diferentes tipos de dados, formatos e mídias.

Conclui a autora que, à medida que caminhamos na direção de uma rede interoperável de informação em saúde, a definição e as normas para um registro legal devem ser mais uniformes. As leis, regulamentos e normas precisam ser mais consistentes, e os softwares de EHRs devem obedecer a um padrão mínimo. Isso irá reduzir o risco, poupará tempo e dinheiro das indústrias e irá trazer mais clareza, necessária para o gerenciamento dos e-registros.

08) Kuczynski K; Gibbs-Wahlberg P. HIPAA the health care hippo: despite the rhetoric, is privacy still an issue? Social Work. USA. 2005 Jul.

As Regras de Privacidade da HIPAA, que entraram em vigor, em de 14 de abril de 2003, com uma prorrogação de um ano para pequenos planos de saúde, impunham um conjunto mínimo uniforme de proteções para privacidade de certas informações em posse das "entidades abrangidas" (planos de saúde, câmaras de assistência à saúde e os prestadores de assistência à saúde), estabelecendo normas para o uso e para a divulgação de todas as informações que dizem respeito ao estado de saúde, prestação ou o pagamento da assistência à saúde, que possam estar ligados a um indivíduo (Informações Protegidas em Saúde) e detidas por uma entidade abrangida.

Baseados nessa interpretação bastante ampla, que pode incluir qualquer parte do registro médico de um indivíduo ou histórico de pagamento, os autores apresentaram, neste artigo, comentários de diferentes autores, mostrando as preocupações com a privacidade das informações "protegidas" dos pacientes, conseqüência do intercâmbio de dados entre operadoras prestadoras de serviços de saúde, necessário para a integração e interoperabilidade dos Sistemas de Saúde, estabelecido pela Lei de Responsabilidade e Portabilidade dos Seguros de Saúde (*Public Law 104-191, Aug. 21 1996, Health Insurance Portability and Accountability Act – HIPAA of 1996*).

Contrários à euforia (em inglês *hype HIPAA*) causada pelas regras de privacidade da HIPAA, os críticos alegavam que, esta lei federal corrói o direito do paciente à privacidade.

Segundo um comunicado emitido pelo grupo Cidadãos para a Saúde, virtualmente toda a informação pessoal da saúde sobre cada aspecto da vida de um indivíduo poderia ser usada e divulgada rotineiramente sem observação, sem o consentimento do indivíduo e de encontro à sua vontade (Dougherty, 2003).

Ressaltava que a privacidade e a confidencialidade estavam correndo um risco, maior do que nunca, por causa de duas questões de segurança inerentes e em conformidade com as regras da HIPAA.

A primeira questão de segurança derivava do fato dos fornecedores de serviços de saúde estarem forçados a usar a Internet para compartilhar a informação e para finalidades do faturamento. As principais críticas apresentadas pelos autores para esta questão são:

Em primeira instância, a confidencialidade do paciente é comprometida pelo governo federal, profissionais de saúde, hackers e pelo sistema jurídico. O governo federal realiza uma economia de bilhões de dólares de imposto pela informatização dos programas Medicare e Medicaid e a HIPAA, e, exceto nas práticas muito pequenas, torna obrigatório o faturamento eletrônico.

A distribuição das informações se amplia através da Internet, sendo essas informações mais fáceis de tornarem-se públicas (Aaronson, 2002). Com a data de nascimento, o sexo e os códigos postais cinco-digitos, 87 por cento da população dos Estados Unidos podem ser identificados (Aaronson).

Os exemplos de violações da segurança do computador e de perdas financeiras associadas têm subido nos últimos anos (Raul, Volpe, & Meyer, 2001). Existem programas informatizados para quebrar senhas, em que nos primeiros 20 minutos de uma tentativa de invasão a uma base de dados, de 20 por cento a 50 por cento das senhas do Windows Microsoft, de uma corporação com 10.000 empregados poderiam ser encontradas, e 90 por cento poderiam ser encontradas dentro de 24 horas “adicionando um ataque de força bruta” (Lee, 2001).

Falhas (*Glitches*) ocorrem nos principais sistemas de computador de uma empresa, implicando a divulgação, não intencional, de informações confidenciais (Raul e outros 2001). Em agosto de 2000, a confidencialidade de 858 pacientes da *Kaiser Permanente* foi violada quando uma falha de computador fez nomeações incorretas (Dyer, 2001). Até agora

nenhum tribunal dos Estados Unidos abordou a questão da falta de responsabilidade com a proteção de um computador de forma adequada (Personick & Patterson, 2003).

O público não tem como recorrer judicialmente sob a nova regra da privacidade (Peisert, 1999). A HIPAA ameaça com sanções ao descumprimento dos regulamentos de segurança, mas se *hackers* ou outros obtiverem informações particulares e um indivíduo for prejudicado, processar pelos tribunais não parece ser uma boa opção. Pelo contrário, se o direito de recusar o compartilhamento de informação só vem a partir da regulamentação da privacidade da HIPAA, o consumidor só pode queixar-se ao Departamento de Saúde e Serviços Humanos (HHS), entrar na fila atrás de milhares de outras pessoas para ver se o organismo irá buscar seus interesses (Privacilla.org, 2003).

A segunda questão de segurança é a introdução do acesso à informação confidencial da saúde, facilitada pela identificação nacional de saúde. O vínculo nacional de todos os registros médicos é possível com tais identificadores (Gelman, Pollack, & Weiner, 1999). Ao contrário das intenções alegadas pela HIPAA, a informação pode ser compartilhada sem o consentimento do paciente e com as emendas de 2003, também pode ser compartilhada, apesar das objeções dos pacientes. As principais críticas apresentadas pelos autores para esta questão são:

Peter Kavanaugh, ex-presidente da Academia para o Estudo das Artes de Psicanálise, afirmou que a diretoria da Academia opõe-se ao novo Juramento HIPAA-crático, que exige o registro de informações pessoais e privadas em uma base de dados nacional informatizada, na qual possa ser acessado por dezenas de agências do governo, milhares de burocratas, corporações farmacêuticas, empresas de seguros privados, agências policiais, funcionários do governo estrangeiro e outros, sem o consentimento da pessoa.

Estudos em saúde e o mercado da droga são os exemplos em que os dados dos pacientes são compartilhados (Aaronson, 2002). O acesso dos agentes policiais à informação médica dos pacientes foi ampliado (Gelman et al., 1999). As atividades em pública podem necessitar da recuperação da informação individualmente identificável, incluindo a informação genética, sem incomodar-se de pedir o consentimento do individual (Peisert, 1999).

Concluem os autores que as preocupações com a HIPAA e a confidencialidade do cliente precisam ser destacadas pelas organizações profissionais para que seus membros

tornem-se conscientes do possível impacto de certas regulamentações da HIPAA e sobre as suas práticas.

Esforços e tempo necessários devem ser concentrados numa avaliação do conteúdo e no tipo de informação em saúde identificável que são compartilhados pela gestão assistencial e as companhias de seguros. Os profissionais precisam manter dossiês (em papel ou eletrônico) que protejam os seus clientes de danos.

Finalmente, energia e dinheiro, também, devem ser direcionados para as ações nos tribunais federais, como por exemplo, o caso dos Cidadãos para a Saúde *versus* Tommy Thompson (Secretario do Departamento de Saúde e Serviços Humanos dos Estados Unidos - HHS), que impõe a regulamentação HIPAA e que expõe a confidencialidade das informações médicas privadas.

09) Hutchon D. Authorised clinical staff need access to clinical information. British Medical Journal (Clinical research ed.). England. 2002 Jan.

Hutchon D. *et al*, alertam neste artigo, como é difícil assegurar os níveis adequados de confidencialidade, exigidos para os sistemas eletrônicos de informação, sem comprometer os serviços essenciais de saúde. A afirmação, "O corpo clínico autorizado precisa de acesso à informação clínica", é uma critica às integrações de sistemas incompletas, que aumentam o problema da proteção da segurança da informação por senha.

Citam a investigação do projeto de saúde "Rumo a Acreditação e Certificação da Telemática Europeia" (*Towards European accreditation and certification of telematics - TEAC - Health*), que classificou os serviços de informática da saúde em três categorias: (1) software e serviços correlatos; (2) telemedicina; e (3) sites da internet. Para o autor não ficou claro como sistemas totalmente integrados, poderiam conter todos os elementos necessários para atender à estratégia da confiança, entretanto, concorda que, um sistema central juntamente com uma série de sistemas sob medida, comunicando-se através de mecanismos de integração, pode fornecer todos esses requisitos, mas ressalva, infelizmente, na minha experiência, a integração nunca é completa, e a proteção de senha é um grande problema.

Numa possível solução para o pronto acesso aos sistemas de informação clínica, pelo corpo clínico autorizado, para Hutchon, essa é uma questão importante que precisa ser resolvida urgentemente, e os requisitos mínimos são: a integração dos serviços (sistemas), com um único logon e uma única senha, e um serviço de assistência telefônica 24 horas que possa, sempre que necessário, ajudar o clínico a lembrar sua senha esquecida.

10) Campos, CJR; Ançäo, MS; Ramos, MP; Sigulem, D. Internet e saúde: aspectos éticos / Internet and health: ethical aspects. Revista brasileira de clínica e terapêutica. Brasil. 2001 Mar.

Os aspectos éticos abordados pelos autores demonstram a preocupação com o uso da Internet na área da saúde, o que tem trazido evidentes benefícios em direção à eqüidade de distribuição do conhecimento, com custo mais baixo que outros meios até hoje utilizados. Embora para eles, tudo terá pouco valor se não for feita uma utilização ética desse conhecimento visando o bem maior de todos os seres humanos, o que se expressa na melhoria da qualidade de vida, em um estado de saúde e em sabedoria, que como citado por Platão, nada mais é do que bem ordenar a própria alma.

Afirmam os autores, "o fundamento da ética médica é o relacionamento médico-paciente". A história, a cultura e as nações têm visto que as pessoas doentes são vulneráveis, dependentes, nervosas, temerosas e passíveis de serem exploradas. Os pacientes, embora hoje menos dependentes do conhecimento técnico acessível, para alguns via Internet, necessitam manter a confiança nessa especial relação (médico-paciente) que se baseia em princípios morais que sempre devem ser o guia do profissional.

Esse artigo apresenta a área da informática em saúde como uma área de caráter multidisciplinar que compreende as seguintes atividades: os *websites* gerais de informação médica e saúde, o desenvolvimento de sistemas de informação hospitalar, as redes de comunicação digital para a saúde, as aplicações voltadas para a saúde comunitária, os sistemas de apoio à decisão, o processamento de imagens e sinais biológicos, a avaliação e controle de qualidade dos serviços de saúde, a Telemedicina, as aplicações voltadas para a área educacional em saúde e o prontuário eletrônico e a área de padrões para a representação da informação em saúde.

Segundo os autores, “a liberdade de uso da Internet é ainda dependente de autorização política de alguns governos totalitários e de condições econômicas favoráveis em alguns países”.

Em suas considerações finais para “Internet e saúde: aspectos éticos”, os autores evidenciam as questões com as seguintes afirmativas:

- Os produtos, serviços e informações referentes à saúde têm o potencial de promover ou prejudicar a saúde. Assim, as organizações e pessoas físicas que proporcionam informações em saúde na Internet têm a obrigação de serem confiáveis, proporcionando conteúdo de alta qualidade, protegendo a privacidade dos usuários e atendo-se às melhores práticas on-line para serviços profissionais e comerciais relativos à saúde.
- Os pacientes têm direito a privacidade que não pode ser infringida sem expresso consentimento esclarecido. Informações que identifiquem o paciente devem ser evitadas, como fichas clínicas e exames subsidiários, a menos que essa informação seja essencial ao propósito da interação com o website e o paciente (ou responsável) forneça consentimento livre e esclarecido.
- Dentre os óbices geralmente apontados pela transmissão de informações médicas na Internet, deve ser ressaltada a questão do sigilo eletrônico. Com base nos conhecimentos atualmente disponíveis, não é possível assegurar proteção total às informações, impedindo seu acesso por outras pessoas.

Concluem que a maneira das pessoas propiciarem e receberem informações e cuidados em saúde está mudando radicalmente com a Internet e, assim, todos os envolvidos nesse processo devem juntar esforços para criar um ambiente seguro e incrementar o valor desse novo veículo para o atendimento das necessidades em saúde.

11) Hodge JG; Gostin LO; Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. Journal of the American Medical Association. USA. 1999 Oct.

"Questões Jurídicas Quanto à Informação Eletrônica em Saúde: Privacidade, Qualidade e Responsabilidade", é um artigo, no qual seus autores apresentaram uma análise das melhorias introduzidas pela tecnologia informatizada (maneira como as informações são coletadas, armazenadas, usadas e divulgadas), no então, moderno sistema de saúde e o conseqüente desafio para as tradicionais proteções jurídicas dos pacientes e prestadores, quanto ao uso e divulgação, das informações em saúde, resumindo em 3 áreas chaves:

1) Privacidade de informações em saúde individualmente identificáveis;
2) Qualidade e confiabilidade das informações;
3) Responsabilidade civil.

Afirmam os autores que proteger a privacidade das informações em saúde (fornecendo algum controle aos indivíduos sobre seus dados em saúde, sem restringir, severamente, o uso autorizado dos dados), diretamente melhora a qualidade e confiabilidade dos dados em saúde (incentivando indivíduos a utilizar plenamente os serviços de saúde e permitindo usos comuns dos dados para o bem social), o que diminui as obrigações da responsabilidade civil (reduzindo as possibilidades de erro médico ou invasões de privacidade individual, melhorando a qualidade e a confiabilidade dos dados de pesquisa em saúde), e finalmente melhora a qualidade dos atendimentos clínicos e medicamentos no mercado.

Na demonstração de sua tese, sobre a questão da privacidade e da tecnologia, apresentaram dois exemplos proeminentes: o e-mail, como meio de comunicação médico-paciente e a prática de telemedicina. Assim, afirmam os autores: "o e-mail pode ser uma ferramenta de comunicação eficaz, no entanto, o uso de correio eletrônico também levanta preocupações de privacidade e segurança".

Em suas análises, para que a utilização de e-mail entre médico-paciente possa refletir os valores da privacidade, exemplificaram com as seguintes orientações da *American Medical Informatics Association*:

1) Obter o consentimento esclarecido do paciente antes de utilizar o e-mail para correspondência direta;

2) Explicar e utilizar mecanismos de segurança;
3) Proibir o encaminhamento do e-mail do paciente sem autorização expressa;
4) Informar aos pacientes sobre aqueles que têm acesso às suas mensagens e se as suas mensagens vão fazer parte do seu prontuário médico;
5) Responder às mensagens de forma responsável;
6) Evitar referências a terceiros.

A Telemedicina melhora o atendimento clínico de populações tradicionalmente carentes (como os pacientes nas áreas rurais), amplia o acesso aos cuidados especiais e tecnologia avançada, e facilita encontros clínicos e atividades educacionais entre médicos e pacientes, também aumentam as possibilidades de invasão de privacidade através da dispersão de dados em saúde por meio de telecomunicações interceptáveis, ampliando assim os riscos de violar o sigilo médico-paciente.

Recomendações semelhantes para a privacidade e proteções de segurança através da criptografia e autenticação de mensagens foram propostas tanto para o e-mail na comunicação médico-paciente, quanto para a prática da Telemedicina.

Na seqüência da análise da interconexão das três áreas (privacidade; qualidade; responsabilidade civil), citadas inicialmente, e da discussão sobre as leis, existentes e propostas, de privacidade das informações em saúde, apresentaram como resumo de suas considerações, as seguintes recomendações para a reforma jurídica sobre a privacidade das informações em saúde:

1) O reconhecimento de informação em saúde identificada como sendo altamente sensíveis;
2) Fornecer garantias de privacidade com base em práticas leais de informação;
3) Habilitar os pacientes com a informação e direitos de consentimento para a divulgação;
4) Limitar a divulgação de dados em saúde em que faltar consentimento;
5) Incorporação de recursos de proteção de segurança;
6) Criação de uma autoridade nacional de proteção de dados;
7) Garantir um nível mínimo nacional de proteção à privacidade.

12) O'Brien DG; Yasnoff WA. Privacy, confidentiality, and security in information systems of state health agencies. American journal of preventive medicine. Netherlands. 1999 May.

Dale G. O'Brien e William A. Yasnoff estavam cientes de que todas as funções essenciais da saúde pública dependem, intrinsecamente, da informação e de que a digitalização, o armazenamento, a transmissão e a proteção da integridade dos dados sensíveis de saúde levantam novas e sérias questões sobre quais pessoas podem acessar esses dados, em quais circunstâncias devem estar disponíveis e como devem ser utilizados de forma adequada.

Assim, propuseram esse estudo em 1999, cujo objetivo foi investigar a privacidade, confidencialidade e a segurança dos sistemas de informação das 50 agências estaduais de saúde do Estados Unidos e os serviços de saúde de Porto Rico e do Distrito de Columbia, seguindo a mesma linha do estudo de 1996, nos Centros de Prevenção e Controle de Doenças (*Centers for Disease Control and Prevention* - CDC), da Infra-estrutura de Telecomunicações da Saúde Pública nas Agências Estaduais da Saúde, que demonstrou o uso generalizado da Tecnologia da Informação nessas agências.

Para fins do estudo, os autores estabeleceram como palavras-chave a privacidade (o direito dos indivíduos para armazenar informações sobre si mesmos, em segredo, sem o conhecimento dos outros), a confidencialidade (a garantia de que as informações identificáveis sobre pessoas, cuja liberação constitua uma invasão da privacidade de qualquer pessoa, não serão divulgadas sem o consentimento, exceto nos casos permitidos por lei) e a segurança dos sistemas de informação (os mecanismos pelos quais políticas de privacidade e confidencialidade são implementadas em computador e sistemas de telecomunicações).

Apesar de citarem algumas leis em seu estudo, para eles enquanto quase todos os estados fornecem alguma proteção legal de informações em saúde mantidas pelo governo, estas leis variam consideravelmente no valor de proteção da privacidade que eles conferem, e constatando a falta de uma lei federal abrangente de proteção da privacidade dos registros médicos, embasaram seu estudo, a partir, de uma expressão menos conhecida, "práticas

justas de informação", que foi codificado em 1973 pelo Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos no relatório intitulado: “Registros, Informática e os direitos dos cidadãos”.

Afirmam os autores que estes princípios têm tido um impacto significativo no desenvolvimento contínuo de uma uniforme política de privacidade federal, promulgados como uma parte da Lei Federal de Privacidade de 1974, a primeira legislação federal do Estados Unidos que abordou especificamente o direito à privacidade, os cinco princípios-chave de “práticas justas de informação” são:

- Nenhum dado pessoal secreto pode existir nos sistemas de manutenção de registros;
- Os indivíduos devem ser capazes de descobrir qual informação pessoal é registrada e como ela é usada;
- Os indivíduos devem ser capazes de impedir que as informações sobre eles obtidas para um propósito, sejam usadas ou disponibilizadas para outros fins, sem seu consentimento;
- Os indivíduos devem ser capazes de corrigir ou alterar um registro de informações sobre si próprios;
- Uma organização criando, mantendo, usando ou divulgando registros de informações pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar precauções razoáveis para evitar a utilização abusiva dos dados.

As Agências Estaduais de Saúde dos Estados Unidos e os Serviços de Saúde do Distrito de Colúmbia e Porto Rico foram entrevistados para coletar dados sobre seus sistemas eletrônicos de informação em saúde.

Um instrumento de pesquisa para avaliar estas questões foi desenvolvido em conjunto com a Associação Estadual e Territorial de Saúde Pública (*Association of State and Territorial Health Officials - ASTHO*) e o Escritório do Programa da Prática de Saúde Pública (*Public Health Practice Program Office - PHPPO*), do CDC. A pesquisa constou de 33 questões em vários formatos, estas questões foram agrupadas nas categorias gerais de

privacidade/confidencialidade e segurança. Várias questões destinadas a obter informações, sobre as práticas corretas de informação, foram agrupadas com as questões de privacidade/confidencialidade.

Concluíram os autores que uma pesquisa dessa natureza é limitada, pela sua orientação essencialmente descritiva, na intensidade das conclusões que podem ser dela extraídas. Qualquer legislação abrangente que for finalmente promulgada deverá fornecer garantias de integridade, disponibilidade e privacidade dos registros em saúde pública.

No final talvez o objetivo definitivo não deva ser a privacidade absoluta, mas dar garantias razoáveis para o público que, quando são recolhidas informações pessoais, as autoridades de saúde pública vão tratar essas informações com respeito, armazená-las em uma forma ordenada e segura, e divulgá-las somente para fins importantes de saúde e em conformidade com os princípios de responsabilidade pública de justiça.

13) Cellini L. Privacy policy. Canadian Medical Association Journal. Canada. 1999 Apr.

Ao comentar o artigo, onde o Dr. Donald J. Willison faz uma boa abordagem do equilíbrio necessário, entre a privacidade das informações dos pacientes e os interesses das seguradoras de saúde e governo, o Dr. Leo Cellini apresenta os direitos dos médicos a serem considerados num ambiente desafiador criado pelas inovações da tecnologia da informação.

A partir de suas indagações: como os médicos podem manter seu papel de "guardiões" das informações, confidenciais e pessoais, de seus pacientes? Qual será o impacto do perfil de médico e das tecnologias de mineração de dados sobre a prática quotidiana da medicina?

Conclui que a questão da privacidade das informações em saúde é talvez mais fundamental para a profissão de medicina do que as outras profissões, tendo em conta as nossas obrigações quando aceitamos o juramento de Hipócrates. Ao considerar as questões de privacidade, devemos nos perguntar se violar confidências é necessário para melhorar o atendimento ao paciente, se há indícios de que vá melhorar os resultados, e como os nossos pacientes se sentem sobre isso. Uma vez que abordando tais questões, poderemos ser

capazes de enfrentar o desafio de Willison de assegurar "a confidencialidade e a segurança das informações utilizadas para a análise da política de saúde e os serviços de saúde".

14) Smith E; Eloff JH. Security in health-care information systems - current trends. International Journal of Medical Informatics. Ireland. 1999 Apr.

Segundo os autores, a possibilidade de maior integração nos sistema de assistência em saúde, impulsionada pelo avanço da Tecnologia da Informação (implementações de prontuários eletrônicos, Intranet e Internet para compartilhar e distribuir as informações em saúde etc), evidenciam a contradição entre a proteção da privacidade dos dados e a necessidade da precisão e da disponibilidade das informações em saúde, para o tratamento adequado dos pacientes (disponibilidade, integridade e confidencialidade).

Nesse artigo, já em 1999, Smith e Ellof buscavam as tendências atuais (da época) para os aspectos de segurança de sistemas de informação em saúde, ou seja, as medidas de proteção para confidencialidade e integridade dos dados eletrônicos dos pacientes, que pudessem garantir o compartilhamento seguro de informações, de natureza extremamente sensível, nos sistemas de saúde.

Citam a evolução do ambiente centralizado, para um cenário distribuído e descentralizado de informações em saúde, focado nas relações custo-beneficio e gestão-qualidade, como um fator de dificuldade para obtenção da segurança dessas informações. O termo cuidado-compartilhado representa o esforço constante e coordenado dos diversos provedores em saúde, visando a proporcionar uma assistência médica, psicológica e social ideal para os seus pacientes.

Afirmam os autores que a proteção da informação se mostra mais difícil de ser conseguida em um ambiente distribuído, do que em um sistema centralizado. Por outro lado, a falha total de um sistema centralizado tem conseqüências muito mais graves, do que uma falha em um ou mais elementos de sistemas distribuídos.

Smith e Ellof estabeleceram o Registro Eletrônico dos Pacientes como meta a ser alcançada pelos profissionais de sistema de informação em saúde e destacaram os diferentes níveis heterogêneos de informatização de registros eletrônicos de pacientes. Os registros eletrônicos em saúde, por exemplo, contêm informações relacionadas

medicamente de um paciente para uma empresa específica, como um hospital, enquanto que o registro eletrônico do paciente contém todas as informações em saúde relacionadas a uma pessoa. Este último, portanto, combina várias bases-empresa de registros eletrônicos em saúde em relação a um paciente. Na verdade a construção do registro eletrônico do paciente exige a integração de informações em saúde através de diversos e diferentes sistemas.

Explicitaram suas preocupações com a segurança do Registro Eletrônico dos Pacientes, apresentando soluções para a não-identificação dos arquivos, eliminando assim os riscos para a confidencialidade de dados em saúde através da utilização de nomes. O registro eletrônico do paciente constitui um passo para o futuro e proporciona aos pacientes uma excelente oportunidade para obter grandes benefícios de cuidados clínicos, pesquisa e prestação de cuidados em saúde. O registro eletrônico de pacientes, no entanto, não será capaz de fornecer estes benefícios a menos que a privacidade do paciente e a confidencialidade possam ser garantidas.

Apresentaram algumas inovações tecnológicas, como os componentes de midllewares (camadas de softwares que concentram serviços como identificação, autenticação, autorização, diretórios, certificados digitais e outras ferramentas para segurança) como solução para a portabilidade e a interoperabilidade desses sistemas distribuídos.

Os principais aspectos de segurança, para armazenamento e transmissão das informações em saúde, abordados pelos autores, nesta visão geral de segurança dos sistemas de informações em saúde, foram: a criptografia, o carro chefe das tecnologias para impedir que terceiros acessem os dados confidenciais dos pacientes; protocolos seguros de rede, para proteção da integridade e confidencialidade nas transmissões de dados usando a Internet; mecanismo de controle de acessos autorizados para proteção das informações sensíveis do paciente; políticas de segurança de bancos de dados; análise de risco de segurança (ameaças, vulnerabilidades e impactos) e as questões jurídicas.

15) Kohane IS; Dong H; Szolovits P. Health information identification and de-identification toolkit. Proceedings American Medical Informatics Association (AMIA) Symposium. USA. 1998.

O projeto de lei dos senadores Edward Kennedy e Nancy Kassebaum (Kennedy-Kassebaum bill), assinado em agosto de 1996, pelo presidente Clinton, garantindo a portabilidade e a responsabilidade dos seguros de saúde dos Estados Unidos, estabeleceu uma discussão para os identificadores nacionais de saúde.

Segundo Kohane e Dong várias propostas foram feitas para adotar ou adaptar um dos vários sistemas de identificação existentes. Entre as propostas mais citadas está aquela da utilização do *Social Security Number (SSN)*, ou de uma simples modificação do mesmo (para inclusão do dígito verificador), como a única abordagem prática que pode tornar possível à adoção em curto prazo o compartilhamento da informação em larga escala pelos sistemas. Os defensores da utilização do SSN descrevem suas vantagens e custo-eficácia como esmagadora, ao contrário, vários estudos nacionais têm alertado contra a aprovação do SSN, e defensores da privacidade quase universalmente se opõem à idéia. No entanto, algumas organizações responsáveis e influentes endossam e estão trabalhando ativamente para assegurar sua adoção.

Nesse texto os autores descreveram o gerador de identificação de sistemas em saúde, a partir (apenas o módulo de identificação) de um trabalho denominado Ferramenta de identificação e de-identificação para sistemas em saúde, em inglês, H*ealth Information Identification and De-Identification Toolkit (HIIDIT)*, financiado pela Biblioteca Nacional de Medicina. Baseado em técnicas de criptografias básicas, consiste em uma tentativa para interligar os registros dos pacientes, através de múltiplas instituições, com a devida autorização. Para os autores antes de pagar o custo da confidencialidade perdida, temos de explorar alternativas técnicas que permitam fácil acesso aos dados, mas ainda proteger a privacidade.

Destacaram as limitações desta abordagem para a proteção da privacidade e apresentaram como exemplo de aplicação, um projeto regional de base de dados de genomas, com preocupações com a confidencialidade das informações, para ilustrar a capacidade e também as limitações do HIIDIT. Esses dados podem prever com precisão os

riscos que um paciente e os outros em sua família podem ter ou de desenvolver doenças graves (e dispendiosas), e essas previsões podem ocorrer sem o consentimento do paciente (ou de seus familiares) para a doação e a análise de seu DNA.

O HIIDIT traz em seus principais conceitos a origem de um sistema de assinatura digital, através de algumas dimensões de propriedades:

- Diretório local: diretório de vínculo dos pacientes com as instituições;
- Escopo de Identificação: representa duas dimensões ortogonais, o âmbito geográfico de organização da identificação (por exemplo, um estudo nacional ou institucional) e da natureza dos dados relacionados com um identificador específico (por exemplo, o registro inteiro do paciente, informações de faturamento, história sexual, ou simplesmente o endereço);
- Autoridade Certificadora: atesta com diferentes graus de autoridade e credibilidade, que o identificador de fato corresponde a um paciente em particular;
- Escopo do Sigilo do Identificador: para quem e o quanto é importante manter um identificador de paciente confidencial;
- Infra-estrutura de criptografia: base de serviços de criptografia.

Permitindo aos projetistas de sistemas definirem o conjunto de concessões desejadas por qualquer sistema específico de informação sobre saúde, proporcionando o compartilhamento dos dados sem comprometer o que de certa forma, as instituições acreditam ser sua propriedade intelectual e os dados confidenciais de seus pacientes.

Concluem os autores que embora o projeto inicial de HIIDIT ser motivado pelo debate nacional sobre os identificadores de saúde universal, a capacidade de HIIDIT ser configurado para atender a uma variedade de objetivos políticos, sugere uma ampla aplicabilidade. Por exemplo, HIIDIT pode ser usado para configurar os sistemas de identificação das bases de dados altamente sensíveis, quer eles incluam dados de genomas ou de história social.

16) France FH. Ethics and biomedical information. International Journal of Medical Informatics. Ireland. 1998 Mar.

Francis H. Roger France nesse texto, Ética e informação biomédica, expressou sua preocupação com a sensibilidade da natureza das informações biomédicas. A divulgação de informações sigilosas sobre defeitos genéticos, comportamentos sexuais e doenças debilitantes poderia não só criar constrangimentos pessoais, mas também discriminações sociais, levando à perda de empregos ou ao fim de casamentos.

Cita o Conselho Geral de Medicina no Reino Unido e os Conselhos de Ética Médica da Bélgica e da França, definindo:

Os médicos são os principais responsáveis pelas informações dadas a eles, pelos pacientes ou obtidas em confiança junto aos pacientes, devendo, portanto, assegurarem que, na medida em que os registros que se encontram sob o seu controle, manual ou informatizado, armazenados ou transmitidos, estejam protegidos por sistemas de segurança eficazes utilizando os procedimentos adequados para evitar a divulgação indevida.

A deontologia médica (um conjunto de princípios, regras e condutas da ética médica tradicional, com base no juramento de Hipócrates, que qualquer médico deve observar, ou ser inspirado, durante o exercício de sua profissão) pode ser utilizada como complemento das leis, ou de contratos específicos entre médicos ou estabelecimentos de saúde e os responsáveis dos dados, sempre que as informações biomédicas forem identificadas e processadas fora do escopo ou do controle da responsabilidade dos profissionais de saúde.

Em suas argumentações, ressaltou a relação médico-paciente como um contrato de respeito ao sigilo das informações médicas, em contradição com a necessidade da disponibilidade e da integridade dessas informações, para a continuidade dos cuidados em saúde.

Para France, privacidade não é sobre informação, é sobre o relacionamento. A questão ética, portanto, não é sobre informação, mas sobre a relação (quais informações, sobre quem, para que propósito, perguntado por quem, a quem enviou, garantiu como e por quem durante a transferência, e mantidos sob a responsabilidade de qual banco de dados?). Relacionamentos implicam em pessoas identificadas. O sigilo não se preocupa com dados anônimos, que não pode ser relacionada a qualquer indivíduo.

Segundo o autor, curiosamente a cultura latina fala principalmente sobre o sigilo das informações médicas pessoais, enquanto no mundo anglo-saxão, o direito à privacidade é o principal objetivo. Um segredo é mantido, principalmente entre dois indivíduos, enquanto os direitos de privacidade implicam em políticas e leis. A confidencialidade é um conceito ético que regulamenta a comunicação de informações entre os indivíduos.

Citou a política de segurança rigorosa desenvolvida no complexo e heterogêneo ambiente de computadores e sistema de rede do Hospital St Luc, em Bruxelas, como exemplo de regras simples e claramente estabelecidas para recuperar a informação médica. Acessos de dados biomédicos identificáveis devem ser reservados para aqueles que têm "o direito de saber" e para um propósito bem definido. Conclui que a ética médica tradicional, com base no juramento de Hipócrates, poderá fornecer orientações adequadas para o exercício das profissões de saúde.

17) Bakker A. Security in perspective; luxury or must? *International Journal of Medical Informatics. Ireland.* 1998 Mar.

Segurança em perspectiva; luxo ou necessidade?

Neste trabalho divulgado há mais de uma década, a segurança em sistemas de informação em saúde é colocada em perspectiva. A maior penetração da tecnologia da informação nos cuidados em saúde é discutida. No uso generalizado da Tecnologia da Informação (TI) nos cuidados em saúde é de vital importância que os computadores possam ser confiáveis em matéria de confidencialidade.

Para Bakker, com a rápida evolução desta tecnologia, vemos cada vez mais sucesso na utilização de cuidados em saúde. Inicialmente, em departamentos isolados, como laboratórios, radiologia ou de administração de registros médicos e, mais tarde, em toda a instituição com os sistemas integrados de informação hospitalar.

Segundo o autor, foi reconhecido no final da década de 1970 que o uso de Tecnologia da Informação e Comunicação (TIC), nos cuidados em saúde, também pode ter efeitos secundários negativos:

- Acesso aos dados do paciente por pessoas não autorizadas;
- A ligação de conjuntos de dados;

- Análise sistemática das bases de dados;
- Perda ou imprecisão dos dados.

Este documento salienta a necessidade de prestar atenção à segurança e sugere uma abordagem responsável com a implementação de medidas técnicas e organizativas. Enfatizou a confusão da diversidade da terminologia da segurança, para os não-especialistas:

- Proteção de dados;
- Privacidade;
- Confidencialidade;
- Integridade de dados, software e utilização;
- Sigilo;
- Segurança;
- etc.

Felizmente, para Bakker, uma terminologia padrão emergiu, dividindo-se o domínio da segurança em três domínios:

- Confidencialidade: A prevenção da divulgação não autorizada de informações;
- Integridade: A prevenção da modificação não autorizada de informações;
- Disponibilidade: A prevenção da retenção não autorizada de informações ou recursos.

Conclui o autor que os sistemas de informação já se tornaram um componente vital, não só para a logística da instituição de saúde, mas também para a prestação de cuidados em saúde e cura. Os cuidados em saúde dependem muito de dados adequados, deste modo a confidencialidade, a disponibilidade e também a integridade são igualmente importantes.

Tendo em vista a natureza muito sensível dos dados do paciente, a importância da confidencialidade foi reconhecida muito antes de os computadores serem inventados. Para o uso generalizado de TI nos cuidados em saúde é de importância vital que os computadores possam ser confiáveis em relação a confidencialidade.

Análise dos Dados

A análise dos artigos, segundo os aspectos dos Sistemas de Informação e da Segurança das Informações em Saúde, gerou a matriz comparativa (Tabela 1) que segue abaixo. Foi elaborada de acordo com as estratégias descritas na metodologia, abordando os enfoques da Privacidade, da Confidencialidade e Consentimento Esclarecido, e também evidenciando suas aplicações nos Registros Eletrônicos em Saúde (RES) e/ou Prontuários Eletrônicos do Paciente (PEP) e nas Trocas de Informações em Saúde (TIS).

Matriz comparativa

Segurança das Informações em Saúde					
Artigos	**Conceitos**			**Aplicações**	
Autor (somente 1º autor)	**Confidencialidade**	**Privacidade**	**Consentimento Esclarecido**	**RES / PEP**	**TIS**
01- Conn, J. (2008)		**X**			**X**
02- Myers, J. (2008)	**X**	**X**			**X**
03- Wiljer, D. (2008)	**X**	**X**		**X**	**X**
04- Boyd, AD. (2007)		**X**			**X**
05- Boyd, KM. (2007)			**X**		**X**
06 - Dallary, SG. (2007)	**X**	**X**			
07- Kloss, L. (2005)				**X**	**X**
08- Kuczynski, K. (2005)	**X**	**X**			**X**
09- Hutchon, D. (2002)	**X**			**X**	
10- Campos, CJR. (2001)	**X**	**X**	**X**	**X**	**X**
11- Hodge, JG. (1999)	**X**	**X**	**X**		
12- O'Bryan, DG. (1999)	**X**	**X**	**X**		
13- Cellini, L. (1999)	**X**	**X**			
14- Smith, E. (1999)	**X**	**X**		**X**	**X**
15- Kohane, IS. (1998)	**X**	**X**	**X**	**X**	
16- France, FH. (1998)	**X**	**X**	**X**	**X**	
17- Bakker, A. (1998)	**X**	**X**	**X**	**X**	**X**

Tabela 1: Matriz comparativa

Recorte por ano e país de publicação:

O início do período foi bastante rico para pesquisa, ou seja, há mais de 10 anos. Poderíamos ter retroagido a 1996, o ano previsto para início do projeto do Cartão Nacional de Saúde, embora o ano de 1998 tenha se revelado uma boa escolha, aproximando a implantação do seu projeto piloto (meados de 1999), com o inicio da nossa pesquisa.

Dos 17 artigos selecionados, 23% foram publicados no ano de 1999, seguidos de 18% nos anos de 1998 e 2007 e 17% em 2008 (Fig. 1).

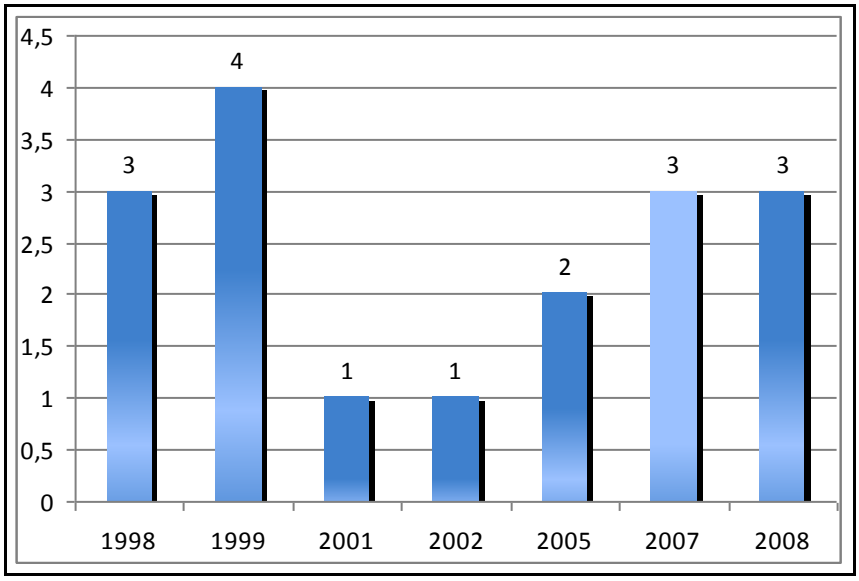

Figura 1 – Distribuição dos artigos selecionados por ano de publicação.

Com relação à distribuição dos artigos por país de publicação observa-se que 7 deles foram publicados no Canadá, 4 na Irlanda, 2 na Inglaterra, 2 no Brasil, 1 na Holanda e 1 no Canadá (Fig. 2).

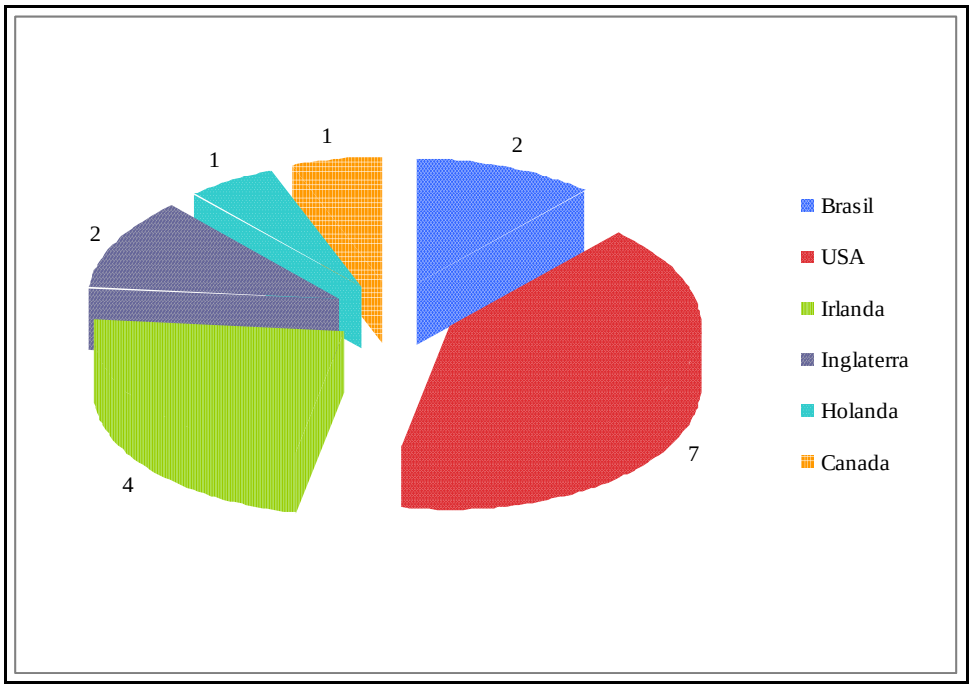

Figura 2: Distribuição de artigos por país de publicação.

Dos conceitos e das aplicações

Ao olhar para a matriz comparativa considerando os temas isolados, segundo o enfoque desta dissertação, 12 autores escreveram sobre Confidencialidade; 14 sobre Privacidade; 7 sobre Consentimento Esclarecido; 8 sobre RES / PEP e 10 sobre TIS. A segurança das informações em saúde é a interseção entre todos os textos.

Segundo esta análise, somente os artigos 10- Campos, CJR. (2001) e 17- Bakker, A. (1998) abordam os três conceitos (Confidencialidade, Privacidade e Consentimento Esclarecido) e os aspectos das duas aplicações (RES / PEP e TIS). No caso das exceções, considerando os conceitos, apenas o artigo 7- Kloss, L. (2005) não aborda nenhum deles e no caso das aplicações, 6 - Dallary**,** SG. (2007), 11- Hodge, JG. (1999), 12- O'Bryan, DG. (1999) e 13- Cellini, L. (1999), não mencionam nem RES / PEP, nem TIS.

Analisando os 16 artigos que trabalham os conceitos da Segurança da Informação em Saúde, constatou-se que 6 artigos analisam os 3 conceitos – confidencialidade, privacidade e consentimento esclarecido, 12 artigos discutem confidencialidade e privacidade e que 01- Conn, J. (2008) e 04- Boyd, AD. (2007) abordam a privacidade, 05- Boyd, KM. (2007) o consentimento esclarecido e 09- Hutchon, D. (2002) apenas a confidencialidade (Fig. 3).

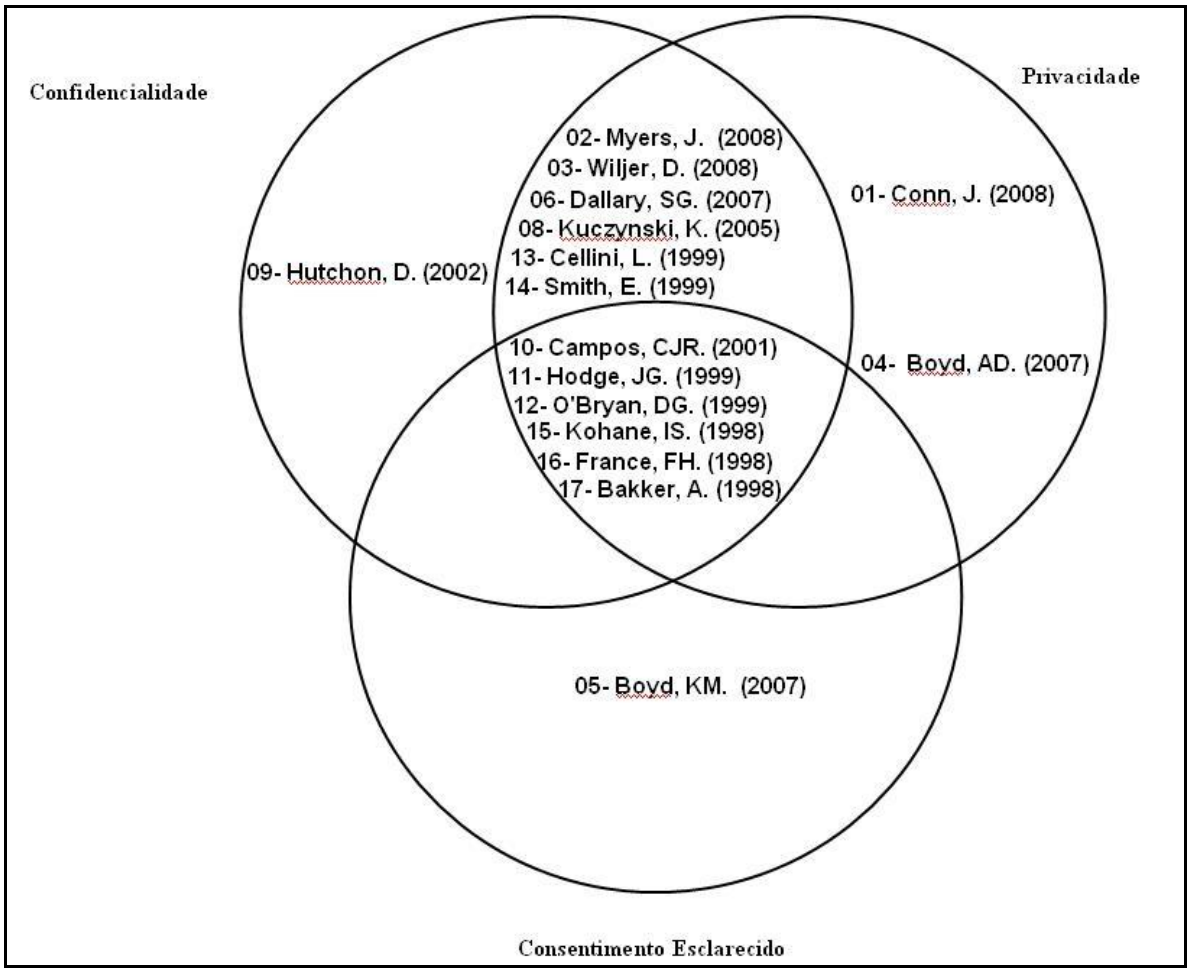

Figura 3: Artigos que trabalham os conceitos da Segurança da Informação em Saúde.

Do mesmo modo para os 13 artigos que analisam os aspectos da segurança para o compartilhamento das informações em saúde, 5 artigos discutem RES / PEP e TIS, 3 somente RES / PEP e 5 trabalham apenas TIS.

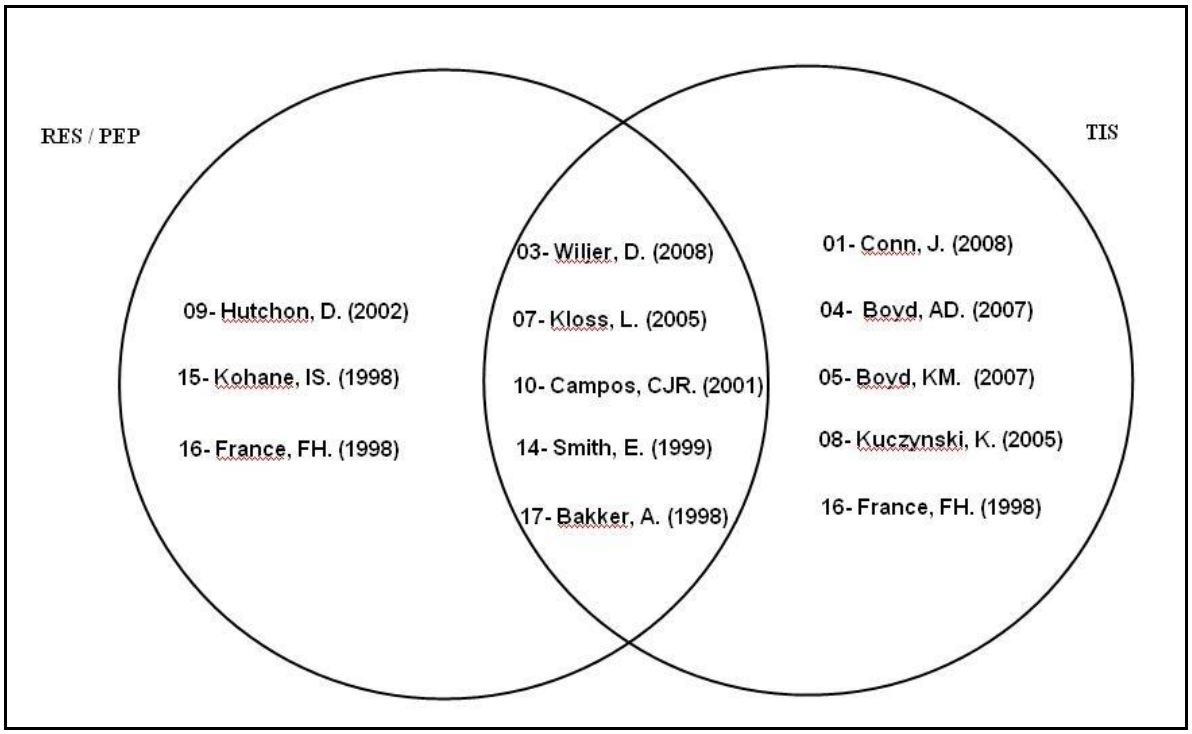

Figura 4: artigos que analisam os aspectos da segurança para o compartilhamento das informações em saúde.

A Segurança da Informação do Sistema de Gerenciamento de Informações Locais (GIL).

A análise da segurança das informações do GIL, baseadas nos conceitos aqui estudados e de acordo com os conceitos estabelecidos pelas normas da ABNT, NBR ISO/IEC 27001:2006 [1], que caracterizam a segurança das informações pela preservação de confidencialidade, integridade e disponibilidade, permite concluir que a segurança das informações do GIL é uma constatação da afirmativa do Ministro Relator Marcos Vilaça, no acórdão 261/2004 do TCU [33], "... não existe, atualmente, procedimentos formais que implementem uma política de segurança adequada no órgão...".

Começando pela integridade, o sistema disponibiliza a função cópia de segurança, que tem por objetivo gerar e/ou restaurar uma cópia de segurança da base de dados com toda a produção da(s) unidade(s) existente(s), sendo sugerido que essa cópia de segurança seja feita ao final de cada dia de trabalho. A validação dos dados digitados realizada através das tabelas internas integradas com os demais sistemas da atenção básica, também auxilia na manutenção da integridade das informações.

A tecnologia de desenvolvimento do GIL garante sua disponibilidade de acordo com a capacidade dos Estabelecimentos Assistências de Saúde (EAS). O sistema pode ser implantado descentralizado nos EAS, com uma configuração mínima sugerida, para seu melhor funcionamento, composta de três equipamentos (um na recepção/arquivo para cadastramento do atendimento, outro no ambulatório de vacinas e o terceiro na administração para digitação da produção) ou até mesmo "*stand-alone*" (uma única maquina). Dependendo do grau de conectividade das Secretarias Municipais de Saúde (SMS) a configuração de implantação pode utilizar o conceito de cliente-servidor, montando uma rede integrada na Secretaria Municipal de Saúde, que receberia informações dos vários EAS de seu município.

A privacidade das informações é garantida pelas rotinas de acesso do sistema, ou seja, somente pessoas devidamente autorizados poderão se conectar, ter acesso às funcionalidades do GIL e realizarem os procedimentos pertinentes às suas funções nos EAS. No cadastramento de usuários, realizado apenas por operadores com perfil de diretor ou administrador (acesso irrestrito), determina-se quais as funcionalidades do sistema que esses usuários encontrarão disponíveis para realizarem as suas atividades.

As recomendações de segurança dos EAS, que se encarregam (ou não) de alertar a equipe multidisciplinar que tem acesso às informações geradas pelo GIL, sobre o caráter legal do sigilo das informações dos pacientes, atualmente se constituem no único mecanismo disponível em busca da confidencialidade das informações.

Algumas instituições possuem um Termo de Confidencialidade, que é submetido aos profissionais que entrarão em contato com registros em saúde dos pacientes (papel ou meios eletrônicos). Através da leitura e assinatura deste documento, garante-se o conhecimento dos aspectos legais para a preservação da confidencialidade e dos deveres sobre o sigilo das informações adquiridas sob o exercício de suas funções em um EAS.

Desta forma, conclui-se de acordo com o voto do Ministro Relator na auditoria solicitada, ao TCU, pelo presidente do DATASUS, para a verificação dos aspectos de segurança, qualidade e controles dos sistemas de processamento de dados, *"... é necessário, portanto, que o DATASUS continue aprimorando a segurança das informações sob a sua custódia, pois, apesar de ter sido constatada a existência de iniciativas isoladas tanto no aspecto da segurança física quanto de acesso lógico..."* [33].

As Propostas

Todos os textos analisados continham aspectos para a segurança das informações em saúde. Alguns que já fazem parte das medidas adotadas, outros que podem ser implementados na iminente Política de Segurança da Informação do DATASUS. A seguir estão listadas as principais contribuições, resultantes da análise do material colhido neste levantamento bibliográfico, sem a pretensão de serem definitivas, sabendo que há exceções que devem ser consideradas:

1) Para privacidade, restringindo os acessos não autorizados das informações em saúde:

- As informações devem ser agrupadas em diferentes níveis de privacidade, os dados identificadores devem ser separados e um controle de acesso deve ser estabelecido para cada nível.
- Mecanismos de acesso restrito com limitações diferenciadas para cada perfil de usuário, de acordo com a sua função, horário e local, para acessar os registros eletrônicos em sua totalidade ou apenas a algumas partes deles.
- Histórico de todas as transações realizadas identificando o que, quem, quando e onde foram acessadas as informações dos pacientes.
- Homologação e/ou certificação dos níveis de segurança dos sistemas (internos ou externos) de informações em saúde.

2) Para a confidencialidade, garantindo a manipulação dos registros eletrônicos em saúde e troca e informações em saúde necessárias para implantação do prontuário eletrônico do paciente:

- Obtenção do consentimento esclarecido, junto ao paciente para o acesso ao seu prontuário eletrônico, especificando os profissionais de saúde, envolvidos na atenção integral da sua saúde.
- Consentimento esclarecido para o uso, processamento e liberação de dados identificados para: as operadoras de planos de saúde, órgãos governamentais, instituições de ensino e pesquisa e os diversos prestadores da atenção à saúde, exceto nos casos excepcionais previsto em lei.
- Mecanismo para o paciente verificar a lista dos acessos ao seu prontuário eletrônico, assim como às operações que foram efetuadas.
- Acesso para o paciente identificar as correções que identifique como necessárias em seus prontuários eletrônicos.
- Garantia do uso devido na liberação de informações para entidades pertencentes ao sistema de saúde, acompanhando a disponibilização e a disseminação dessas informações.

3) Para a classificação do nível de segurança das informações:

- Devido a sua natureza sensível e aos danos potenciais que podem ser causados por mau uso ou divulgação, quaisquer informações em saúde devem ser consideradas como confidenciais.

Classificar como confidencial somente a informação sem identificação, é insuficiente. Para D'Ornellas e Rocha [4], "sistemas que possuem acesso restrito e até mesmo sistemas que não fornecem qualquer tipo de identificação sobre pacientes específicos podem ser manipulados para produzir informações médicas sobre indivíduos específicos".

Conclusão

Mais do que demonstrar a inter-relação dos termos escolhidos para esta dissertação, o presente levantamento bibliográfico revelou que a segurança das informações em saúde, com enfoque da privacidade e da confidencialidade, implica diretamente no respeito do principio da autonomia, e que este deve ser expresso na adoção de regras para a obtenção do consentimento esclarecido, fornecendo aos pacientes garantias contra o uso indevido de suas informações em saúde.

A afirmativa de que "privacidade não é sobre a informação, é sobre o relacionamento" (France FH, 1998), valida a diferença estabelecida por esta dissertação para os termos privacidade e confidencialidade. Interliga a segurança das informações em saúde com os aspectos éticos na relação entre paciente e os profissionais de saúde, evidencia a necessidade de acessos diferenciados aos prontuários do paciente e a obtenção do consentimento esclarecido dos pacientes, para uso de suas informações em saúde.

Ainda com base na pesquisa, o texto de Wiljer D. et all, 2008, fundamenta que: "soluções flexíveis, padronizadas e interoperáveis são necessárias para assegurar aos PAEHRs, suporte de atendimento integrado e global. Proporcionar o acesso aos EHRs, é uma etapa essencial na ativação da assistência dos pacientes e na melhoria em ampla escala do sistema de saúde".

O cruzamento dos termos sistema de informação e segurança das informações em saúde, nas bases de dados MEDLINE e LILACS, possibilitou, na análise do presente levantamento bibliográfico, ressaltar a importância os aspectos da privacidade, da confidencialidade e do consentimento esclarecido, na obtenção e na garantia da interoperabilidade necessária para a troca das informações entre os sistemas informatizados em saúde.

Finalmente, segurança da informação para a troca das informações em saúde é a base para a implantação do Prontuário Eletrônico do Paciente um objeto que, em 2008, Vasconcellos [47], evidenciou como, "estratégico para a decisão clínica e gerencial, para o apoio à pesquisa e formação profissional e critério de avaliação da qualidade da prestação de serviço de saúde".

6. Considerações Finais.

Considerando-se que o objetivo principal desta dissertação centra-se na expressão dos conceitos da privacidade e confidencialidade no contexto dos Registros Eletrônicos em Saúde (RES), durante toda a trajetória da pesquisa buscou-se a compreensão desses conceitos sob diferentes enfoques e abordagens.

Por tratar-se de um tema ainda pouco explorado pelas pesquisas acadêmicas e com pouca literatura disponível, partiu-se para analisar artigos científicos, de acordo com o estabelecido na metodologia, de forma a apreender o que está sendo concebido em diferentes países, no tocante á temática de interesse. Desta forma, a análise dos conteúdos dos textos aqui apresentados, permite chegar a algumas conclusões.

A partir da pesquisa aqui empreendida, conclui-se que os conceitos diferenciados de privacidade e confidencialidade das informações em saúde fazem parte da segurança dos SIS. E que essa é uma questão bastante complexa na medida em que envolve vários atores como pacientes, médicos, outros profissionais da saúde e os profissionais de informática em saúde.

É fato que o desenvolvimento e expansão das tecnologias de informação e comunicação, sobretudo no momento de chegada às redes sociais (ou da sociedade em rede?), foram responsáveis por um novo paradigma informacional. Desafios e dilemas passaram a ter de ser enfrentados pela gestão dos registros em saúde. Um destes diz respeito à proteção do paciente e à necessidade de disponibilizar suas informações em saúde, uma vez que dessa dicotomia poderão resultar benefícios para o próprio paciente e para os demais cidadãos.

Na verdade, é de tal ordem complexo que se pode perceber, ao analisar os 17 textos, que os focos de atenção vão se alterando ao longo do tempo e de acordo com os desenvolvimentos tecnológicos. Ao final da década de 1990 e início dos anos 2000, a maioria dos textos apresentava preocupações com os acessos não autorizados nas informações em saúde. Já nos anos de 2007 e 2008 as preocupações se voltam, também, para o compartilhamento das informações, consubstanciado nas redes sociais. Desta forma, de acordo com os avanços da Internet, essa evolução é expressa nos termos navegar, recuperar/atualizar, interagir e interoperar, presentes nos textos estudados.

Em sua maioria abordam e preconizam ações, iniciativas que devem preceder a implementação de dispositivos técnicos, que passam pela educação e conscientização dos pacientes sobre a importância em compartilhar de forma consentida suas informações, assim como, treinamento e conscientização, visando a garantir a postura ética dos profissionais que manipulam as informações em saúde, em não expor o paciente.

Pode-se também concluir que a implantação da Política de Segurança da Informação, baseada na implantação de um Sistema de Gestão de Segurança da Informação (SGSI), orientada pela norma ABNT NBR ISO/IEC 27001:2006 [1], capacita o DATASUS de forma necessária, mas não suficiente, para a garantia dos aspectos básicos de confidencialidade, integridade e disponibilidade para proteção da informação sob sua custódia.

Neste enfoque, onde se buscou compreender a distinção entre os conceitos de privacidade e confidencialidade das informações em saúde, foi possível constatar que o aparato tecnológico para controle de acesso (embutidos na implantação do SGSI), estabelece apenas a manutenção de níveis aceitáveis de segurança da informação para a privacidade. Embora a criptografia dos dados e os controles de acesso sirvam também para fornecer alguma garantia para a segurança no compartilhamento das informações em saúde, percebe-se que a tecnologia se mostra insuficiente na garantia da confidencialidade desta tão sensível informação.

A informação em saúde sob a responsabilidade do DATASUS é a mesma obtida em confiança na relação médico-paciente e, não existe nada que a proteja contra a revelação não autorizada. Somente uma estrutura baseada na ética do respeito à confidencialidade, complementada pela obtenção do consentimento esclarecido, pode tentar garantir a privacidade das informações em saúde e estimular a prática ética na relação entre os profissionais, inclusive os de informática, e os usuários do sistema de saúde.

7. Referência Bibliográfica.

1. ABNT – Associação Brasileira de Normas Técnicas. NBR ISO /IEC 17799. Disponível em http://www.abnt.org.br. Acessado em dezembro de 2008.

2. KOBAYASHI, L. O. M., FURUIE, S. S. (2007), **Segurança em informações médicas: visão introdutória e panorama atual / Security in medical information: overview and current scenario**, Revista brasileira de engenharia biomédica / Sociedade Brasileira de Engenharia Biomédica; v. 23, n. 1, p. 53-77, abril 2007. Disponível em: http://www.sbeb.org.br/rbeb/indices/rbe_indi.htm. Acessado em Dezembro/2008.

3. FRANCESCONI, C. F., GOLDIM, J. R.. **Aspectos Bioéticos da Confidencialidade e Privacidade** (p. 269 a 284). In Iniciação à Bioética. Org. Costa, Oselka e Garrafa. 1998, 302p.

4. DORNELLAS, M. C., ROCHA, R. P.. **Acesso e Privacidade: Em Busca da Segurança das Informações em Bancos de Dados Médicos**. In: VIII Congresso da Sociedade Brasileira de Informática em Saúde, 2002, NATAL, p. 76-81.

5. RINDFLEISCH, T. C. (1997), **Privacy, information technology, and health care**, Communications of the ACM, v. 40, n. 8, p. 92-100.

6. CUSHMAN, R. (1996), **Information and medical ethics: protecting patient privacy**, IEEE Technology and Society Magazine, v. 15, n. 3, p. 32-39.

7. BRASIL. PRESIDÊNCIA DA REPÚBLICA FEDERATIVA DO BRASIL. **Legislação**. Disponível em: http://www.presidencia.gov.br/legislacao. Acessado em dezembro de 2008.

8. BRASIL. MINISTÉRIO DA SAÚDE. SECRETARIA EXECUTIVA. DEPARTAMENTO DE INFORMÁTICA DO SUS - DATASUS. **O DATASUS**. Disponível em: http://w3.datasus.gov.br/datasus. Acessado em dezembro de 2008.

9. BRASIL. CONSELHO NACIONAL DE SECRETÁRIOS DE SAÚDE; **Ciência e Tecnologia em Saúde**. – Coleção Progestores – Para entender a gestão do SUS, 4; Brasília: CONASS, 2007. Disponível em: http://www.conass.org.br. Acessado em dezembro de 2008.

10. BRASIL. MINISTÉRIO DA SAÚDE. **Trajetória 1991-2002.** Brasília: Ministério da Saúde, 2002. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/trajetoria_datasus.pdf. Acessado em dezembro de 2008.

11. BRASIL. MINISTÉRIO DA SAÚDE. **Política Nacional de Informação e Informática em Saúde. Proposta versão 2.0 (inclui deliberações da XII Conferência Nacional de Saúde)**. 29 de março de 2004. Disponível em: http://portal.saude.gov.br/portal/arquivos/pdf/PoliticaInformacaoSaude29_03_2004.pdf. Acessado em dezembro de 2008.

12. SABBATINI, R. M. E. **História da Informática em Saúde no Brasil; Informática Médica Volume 1 Nº 5**. Set /Out 1998. Disponível em: http://www.informaticamedica.org.br/informaticamedica/n0105/sabbatini.htm. Acessado em Dezembro de 2008.

13. SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE (SBIS). **Informática Médica ou Informática em Saúde** (1986). Disponível em http://www.sbis.org.br. Acessado em Dezembro de 2008.

14. MORAES, I. H. S., 1994. **Informações em saúde: da prática fragmentada ao exercício da cidadania.** SP-RJ: Hucitec/Abrasco.

15. CARVALHO, A. O., PAULA EDUARDO, M. B. **Sistemas de Informação em Saúde para Municípios, volume 6**. São Paulo : Faculdade de Saúde Pública da Universidade de São Paulo, 1998. (Série Saúde & Cidadania) p.17-56. Disponível em http://bvsms.saude.gov.br/bvs/publicacoes/saude_cidadania_volume06.pdf. Acessado em novembro de 2008.

16. CUNHA, R. E. **Cartão Nacional de Saúde: os desafios da concepção e implantação de um sistema nacional de captura de informações de atendimento em saúde**. Ciência saúde coletiva. 2002; 7(4): 869-878. Disponível em: http://www.scielo.br/pdf/csc/v7n4/14610.pdf. Acessado em novembro de 2008.

17. MINISTÉRIO DA SAÚDE, BRASÍLIA. 1996. **Gestão plena com responsabilidade pela saúde do cidadão (Norma Operacional Básica do SUS 01/96)**. Disponível em: http://siops.datasus.gov.br/Documentacao/NOB%2096.pdf. Acessado em Dezembro de 2008.

18. BRASIL. MINISTÉRIO DA SAÚDE. SECRETARIA EXECUTIVA. DEPARTAMENTO DE INFORMÁTICA DO SUS - DATASUS. 1999. **Cartão Nacional de Saúde – Licitação - Downloads**. Disponível em http://www.datasus.gov.br/cartao/edital/download.htm. Acessado em novembro de 2008.

19. MINISTÉRIO DA SAÚDE. GESTÃO DA SAÚDE. **Cartão Nacional de Saúde**. Disponível em http://portal.saude.gov.br/portal/saude/Gestor/area.cfm?id_area=944. Acessado em Dezembro de 2008.

20. MASSAD, E., MARIN, H. F., AZEVEDO N. R. **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico / Eletronic record of pacient care, information and medial knowlegde**. São Paulo; FMUSP/UNIFESP/OPAS. 2003. 202 p. Disponível em http://www.sbis.org.br/site/arquivos/prontuario.pdf. Acessado em novembro de 2009.

21. ROGER, F. F. H, GAUNT, P. N. **The need for security - a clinical view. Int J Biomed Comput**, v. 35, Suppl 1, p. 189-194, 1994.

22. CONSELHO FEDERAL DE MEDICINA – CFM. **Resoluções**. Disponível em http://www.portalmedico.org.br/php/pesquisa_resolucoes.php. Acessado em novembro de 2009.

23. LEÃO, B. F. **Padrões para representar a informação em saúde. In: Seminário Nacional de Informações e Saúde: o setor no contexto da sociedade da informação**. 20 a 23 de novembro de 2000. Rio de Janeiro. Fundação Oswaldo Cruz, 2000, p. 21-34.

24. BRASIL. CONSELHO NACIONAL DE SECRETÁRIOS DE SAÚDE. **Atenção Primária e Promoção da Saúde.** Conselho Nacional de Secretários de Saúde. Brasília. CONASS, 2007. 232 p. (Coleção Progestores – Para entender a gestão do SUS, 8).

25. BRASIL. MINISTÉRIO DA SAÚDE. SECRETARIA EXECUTIVA. DEPARTAMENTO DE INFORMÁTICA DO SUS - DATASUS. **Gerenciador de Informações Locais - GIL**. Disponível em: http://gil.datasus.gov.br. Acessado em setembro de 2009.

26. MORAES I. H. S., GONZÁLES DE GÓMEZ, M. N. G. **As autoras respondem**. Ciência & Saúde Coletiva [online]. 2007, vol.12, n.3, pp. 579-585. ISSN 1413-8123. doi: 10.1590/S1413-81232007000300008.

27. WADLOW, A.T. **Projeto e Gerenciamento de Redes Seguras**; Editora Campus, 2000.

28. IACHELLO, G., ABOWD, G. D. (2005), **Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing**, In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Portland, p. 91-100, 02-07 Apr.

29. PFITZMANN, A., PFITZMANN, B. (1992), **Technical Aspects of Data Protection in Health Care Informatics,** In: Advances in Medical Informatics, Eds.: J. Noothoven van Goor, J.P. Christensen, IOS Press, p. 368-386.

30. GRITZALIS, S., LAMBRINOUDAKIS, C., LEKKAS, D., DEFTEREOS, S. (2005), **"Technical guidelines for enhancing privacy and data protection in modern electronic medical environments"**, *IEEE Transactions on Information Technology in Biomedicine*, v. 9, n. 3, p. 413-423.

31. NIINIMÄKI, J., SAVOLAINEN, M., FORSSTRÖM J. J. (1998), **Methodology for security development of an electronic prescription system**, In: Proceedings of AMIA Symposium, Orlando, p. 245-249, 07-11 Nov.

32. ORGANIZAÇÃO PAN-AMERICANA DE SAÚDE (OPAS), 1999. **Cyberspace Law and Ethics: A Health Sector Perspective**.

33. BRASIL. TRIBUNAL DE CONTAS DA UNIÃO - TCU. **Acórdão 461/2004**. Disponível em http://contas.tcu.gov.br/portaltextual. Portal de Pesquisa Textual. Acessado em dezembro de 2008.

34. BASTOS, A., CAUBIT, R. **ISO 27001 e 27002: Gestão de segurança da informação – uma visão prática**. Porto Alegre, RS; Zouk, p.9-28, 2009.

35. SHORTLIFFE, E. H. (1998), **The evolution of health-care records in the era of the Internet**, In: Proceedings of the 9th World Congress on Medical Informatics [MedInfo98], Seoul, p. 1-8, 18-22 Aug.

36. RAGHUPATHI, W., Tan, J. (2002), **Strategic IT applications in health care**, Communications of the ACM, v. 45 n. 12, p. 56-61.

37. KWAK, Y. S. (2005**). International standards for building Electronic Health Record (EHR), In: Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry** [HEALTHCOM2005], Busan, p. 18-23, 23-25 Jun.

38. SMITH, E., ELOFF, J. H. P. (1999), **Security in health-care information systems – current trends**. International Journal of Medical Informatics, v. 54, n. 1, p. 39-54.

39. LOCH, J. A. **Confidencialidade; natureza, características e limitações no contexto da relação clínica.** Bioética;11(1):51-64, 2003. Disponível em : http://search.bvsalud.org/regional/resources/lil-383346 Acessado em Dezembro de 2008.

40. CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO - CRM-SP. **Juramento de Hipócrates.** Disponível em: http://www.cremesp.org.br/?siteAcao=Historia&esc=3. Acessado em Dezembro/2008.

41. BEAUCHAMPS, T. L. & CHILDRESS, J. F. **Princípios de Ética Biomédica**. (4ª ed.) São Paulo. Edições Loyola. 2002.

42. SÉGUIN, E. **Biodireito**. Rio de Janeiro, Lumens Juris, 2001.

43. KANT, I. **Foundations of the Metaphysiscs of Morals**. trad. Lewis White Beck (Indianapolis, IN:Bobbs-Merril Company, 1959). **The Doctrine of Virtue, parte II de "Metaphysics of Morals"**. trad. Mary Gregor (Philadelphia: University of Pennsylvania Press,1964), esp. P.127.

44. MILL, J. S. **On Liberty**. Collected Works of John Mill, vol.18, caps I, III. Toronto: University of Toronto Press. 1977.

45. NEVES, N. C. **Ética para os futuros médicos: é possível ensinar?** Brasília. Conselho Federal de Medicina, 2006.

46. INTERNATIONAL MEDICAL INFORMATICS ASSOCIATION. **O Código de Ética da IMIA para Profissionais de Informática em Saúde**. Disponível em http://www.imia.org/pubdocs/Portuguese_Translation.pdf. Acessado em Dezembro de 2008.

47. VASCONCELLOS, M. M., GRIBEL, E. B., MORAES, I. H. S. **Registros em saúde: avaliação da qualidade do prontuário do paciente na atenção básica**. Rio de Janeiro, Brasil. Cad. Saúde Pública [online]. 2008. Vol. 24. acessado em Dezembro de 2009. Disponível em: http://www.scielo.br/pdf/csp/v24s1/21.pdf.