XIX SEMEAD
Seminários em Administração
novembro de 2016
ISSN 2177-3866

MECANISMOS DE PROTEÇÃO DE INFORMAÇÕES EM INSTITUIÇÕES DE SAÚDE SOB A ÓTICA DE DOCUMENTOS REGULTATÓRIOS E NORMATIVOS

ODIRLEI ANTONIO MAGNAGNAGNO
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS)
odirleimag@hotmail.com

EDIMARA MEZZOMO LUCIANO
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS)
eluciano@pucrs.br

GUILHERME COSTA WIEDENHÖFT
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS)
wiedenhoft@gmail.com

Introdução
Na busca de melhorar o aspecto da privacidade da informação, as organizações têm se preocupado muito com a adoção de Tecnologias da Informação (TI), com a intenção de gerenciar os seus dados e fornecer um melhor produto ou serviço ao seu cliente de forma segura. Assim como em outros ramos de atividade, no ambiente hospitalar também há uma grande preocupação com a privacidade das informações, e ainda com um agravante, já que as informações relacionadas aos seus clientes são de extrema particularidade, pois envolvem aspectos a respeito de sua saúde e precisam ser protegidas.

Problema de Pesquisa e Objetivo
Este trabalho delimita-se ao seguinte problema de pesquisa: Existem mecanismos registrados em Documentos Regulatórios e Normativos, que possam contribuir com a segurança e privacidade da informação em uma instituição de saúde? O objetivo ao responder essa questão é identificar os mecanismos propostos por documentos Regulatórios e Normativos que possam ser utilizados em instituições de saúde. Especificamente, pretende-se identificar documentos Regulatórios e Normativos que possam conter mecanismos de proteção e classificar os mecanismos encontrados.

Fundamentação Teórica
A fundamentação teórica traz uma abordagem de segurança e privacidade da informação em ambientes hospitalares e uma explanação de documentos Regulatórios e Normativos.

Metodologia
Esta pesquisa se caracteriza como uma pesquisa exploratória de corte transversal com abordagem descritiva, utilizando dados qualitativos. O levantamento bibliográfico foi utilizado como método para a revisão sistemática. Para atender os objetivos foram analisados 20 documentos, qualificando os mecanismos e posteriormente classificando-os por tipo e características.

Análise dos Resultados
Ao término da análise dos artigos e posteriormente os 20 Documentos Regulatórios e Normativos, chegou-se a 37 mecanismos. Para melhor atender ao objetivo da pesquisa, os mecanismos foram agrupados em Mecanismos de Estrutura, Mecanismos de Processo e Mecanismos de Relacionamento. Após a classificação pelo tipo de mecanismos, foi realizada uma classificação conforme o seu eixo de ação, ou seja, vulnerabilidade, salvaguarda, detecção, punição e conscientização.

Conclusão
O artigo traz como resultado principal a implementação do conhecimento com a descrição de mecanismos de privacidade da informação em ambientes hospitalares, assim como a descrição dos documentos regulatórios e normativos que contém esses mecanismos. O resultado da revisão sistemática pode fornecer uma base de documentos para administradores hospitalares e também pesquisadores que embasem práticas que protejam a informações dos pacientes.

Referências Bibliográficas
HERATH, Tejaswini; RAO, H. Raghav. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems, v. 18, n. 2, p. 106-125.
LUCIANO, E. M.; BRAGANÇA, C. E. B. de A.; TESTA, M. G. (2011). Privacidade de informações de pacientes de instituições de saúde: a percepção de profissionais da área de saúde. Reuna (Belo Horizonte), v. 16, p. 89-102.
GOLDIM,J. R.; FRANCISCONI, X. (2004). Bioética Clínica. Disponível em: Acesso em: 25 Jun. 2014.

MECANISMOS DE PROTEÇÃO DE INFORMAÇÕES EM INSTITUIÇÕES DE SAÚDE SOB A ÓTICA DE DOCUMENTOS REGULTATÓRIOS E NORMATIVOS

INTRODUÇÃO

Na busca de melhorar o aspecto da privacidade da informação, as organizações têm se preocupado muito com a adoção de Tecnologias da Informação (TI), com a intenção de gerenciar os seus dados e fornecer um melhor produto ou serviço ao seu cliente de forma segura. Assim como em outros ramos de atividade, no ambiente hospitalar também há uma grande preocupação com a privacidade das informações, e ainda com um agravante, já que as informações relacionadas aos seus clientes são de extrema particularidade, pois envolvem aspectos a respeito de sua saúde. Em muitos casos, como afirmam Acquisti e Grossklags (2007), essa informação que deveria ser protegida pode estar sendo utilizada sem que se saiba onde e como. Justamente informações do prontuário médico, que estão entre os tipos de informações que mais se deseja proteger e preservar (GAERTNER; SILVA, 2005).

Segundo Luciano, Bragança e Testa (2011), os aspectos de privacidade na área da saúde têm relação com o sigilo das informações do prontuário eletrônico, e o comportamento dos profissionais que acessam estas informações constantemente, podendo apresentar diferentes níveis de atitudes em relação às políticas e mecanismos de privacidade de um hospital, devido à individualidade de cada um. É difícil para os hospitais saberem exatamente como garantir a privacidade das informações de uma maneira integra. Um dos meios utilizados, além das políticas de segurança é a criação de normas, que podem ser formais ou informais, que orientem e conscientizem os colaboradores de uma instituição de saúde quanto à privacidade da informação, sendo ela da instituição como um todo, ou especificamente das informações dos pacientes contidas nos prontuários eletrônicos.

Os hospitais não possuem um documento regulatório normativo externo que forneça parâmetros mais diretos para a construção das normas de segurança para a proteção das informações. “O Brasil ainda carece de legislação neste sentido, existindo apenas resolução e normativas dos Conselhos Federal e Estaduais de Medicina, que abordam apenas questões sobre disponibilidade de informações médicas no ambiente hospitalar” (LUCIANO; BRAGANÇA; TESTA, 2011, p. 89).

Face ao exposto acima este trabalho aborda como tema a privacidade das informações, tendo como foco principal a privacidade das informações dos pacientes em instituições de saúde, buscando identificar mecanismos de proteção, através da análise de documentos Regulatórios e Normativos. De forma diferente, os Estados Unidos tem uma preocupação maior com essa questão, pois visam proteger toda informação pessoal disponibilizada e utilizada na prestação de serviços de saúde através da formulação de leis. Entre uma das mais importantes está o *Health Insurance Portability and Accountability Act* (HIPAA). Ações como estas podem se consideradas uma resposta oficial para questões éticas e morais para proteção das informações dos indivíduos, respaldadas pela lei nos Estados Unidos (BAUMER; EARP; PAYTON, 2000). Neste sentido, este trabalho delimita-se ao seguinte problema de pesquisa: Existem mecanismos registrados em Documentos Regulatórios e Normativos, que possam contribuir com a segurança e privacidade da informação em uma instituição de saúde? O objetivo ao responder essa questão é identificar os mecanismos propostos por documentos Regulatórios e Normativos que possam ser utilizados em instituições de saúde. Especificamente, pretende-se identificar documentos Regulatórios e Normativos que possam conter mecanismos de proteção e classificar os mecanismos encontrados, pois o Brasil não conta com uma legislação específica a respeito de privacidade

de informações de saúde, dizendo o que deve se feito para garantir a privacidade das informações dos pacientes. Este artigo faz parte de uma pesquisa mais ampla sobre Privacidade na Área da Saúde.

FUNDAMENTAÇÃO TEÓRICA

Segurança da informação

As normas ISO/IEC 27001:2006 e ISO/IEC 27002:2005, que respectivamente tratam dos requisitos para a gestão da Segurança da Informação e das práticas de sistemas de gestão da Segurança da Informação, as quais buscam melhorar essa gestão através do estabelecimento de diretrizes e princípios para iniciar, programar, manter e aperfeiçoar a gestão da informação nas organizações, são de grande importância quando se trata de segurança da informação.

De acordo com Luciano e Klein (2014), a Segurança da Informação possui três abordagens que atuam em conjunto visando à proteção da informação, que é a abordagem técnica, a abordagem normativa e a abordagem comportamental, que respectivamente representam medidas de proteção com *hardware* e s*oftware*, aderência a normas e regulamentos e o fator comportamental do usuário.

Luciano e Klein (2014) apresentam um conceito da informação, a fim de que ela tenha utilidade. Para isso precisa atender algumas condições e não somente estar disponível para a organização. De acordo com os autores, a informação, desde a sua criação até o seu descarte precisa atender sete requisitos conforme são apresentados no Quadro 1.

Quadro 1
Requisitos da Informação Segura

Requisitos	Contextualização
Confidencialidade	A informação deve ser protegida contra a sua divulgação não autorizada de acordo com o grau de sigilo do seu conteúdo
Integridade	É a validade da informação de acordo com os valores de negócios e expectativas, bem como a exatidão e a completude dos ativos de informações
Disponibilidade	É a garantia da disponibilidade da informação no momento em que se faz necessário
Autenticidade	É o dever de assegurar que a informação é autêntica
Confiabilidade	É a garantia da autoria dos dados
Conformidade	A informação deve ser mantida em conformidade com o ato regulatório da qual foi criada, por exemplo, a política de Segurança da Informação
Irrefutabilidade	É a garantia da impossibilidade de negar a autoria da informação

Fonte: LUCIANO e KLEIN (2014).

O caminho a ser adotado pelas instituições de saúde é reduzir ao máximo quaisquer riscos às informações e manter a integridade e a disponibilidade dos Sistemas de Informação. E para isso é importante fazer uma boa análise de riscos, definindo uma política de segurança dentro e fora da organização (internet, intranet e extranet), buscando como base documentos que possam auxiliar nessa tarefa.

As instruções a respeito de Segurança da Informação podem estar contidas nas políticas de segurança, que têm a função de dar suporte, auxiliar no planejamento de implantação de sistemas, sobre como deve agir cada integrante da equipe de assistência médica e como será abordada a política de segurança. Porém, segundo Bulgurcu et al. (2010), a decorrência da vulnerabilidade vem do funcionário que não segue a Política de Segurança da Informação. De acordo com Vance et al. (2012) a vulnerabilidade é a possibilidade de um incidente indesejado ocorrer caso não tenha medidas para evitá-lo. Com isso, "cada organização deve estabelecer quais políticas serão utilizadas tendo como base suas

necessidades, requisitos legais, cultura interna e sistemas informatizados" (FERREIRA; ARAÚJO, 2008, p. 34).

Contudo, mesmo com as políticas estabelecidas e com as boas práticas divulgadas para se melhorar a Segurança da Informação de um hospital, se o usuário do Sistema de Informação não colaborar e estiver consciente, não terá um bom êxito (BRAGANÇA et al., 2010). Já que essa consciência em relação à informação segura, de acordo com Siponen (2000) é o aumento e o esforço dos resultados das ações realizadas pelas organizações relacionadas à Segurança da Informação, sensibilizando o usuário no cumprimento e bom desempenho, a fim de diminuir as ameaças em relação à Segurança da Informação.

Privacidade da informação em ambientes hospitalares

A NRC (1997) classifica em duas grandes áreas as ameaças com a privacidade do paciente, uma delas é a ameaça sistemática, ou seja, uma intromissão no fluxo da informação, divulgando dados além do necessário. A segunda ameaça se refere ao acesso inadequado aos dados do paciente, tanto por colaboradores que podem se utilizar de privilégios quanto por pessoas externas explorando a vulnerabilidades do Sistema de Informação.

Todos os participantes do processo de registro, armazenamento ou acesso à informação de um prontuário eletrônico tendem, a saber, o valor da informação e a importância de preservá-la. Segundo Luciano e Klein (2014) a informação é utilizada para a tomada de decisões na organização, podendo trazer prejuízos financeiros caso ocorra algum vazamento. Por isso essa informação deve estar sempre protegida e controlada, não importando como está sendo armazenada ou compartilhada (SÊMOLA, 2003).

A privacidade na área hospitalar requer principalmente integridade e proteção de dados, tornando-se particularmente importante devido ao crescimento contínuo da tecnologia (SMITH, 1996). Essa privacidade de informações, conforme coloca Leino Kilpi, et al. (1999) em muitos casos têm a ver com o nível de confiança das informações do paciente, sendo que uma das áreas básicas de privacidade em hospitais está relacionada com a proteção de dados e a prevenção de erros de informação.

O comportamento humano pode gerar possíveis violações na Segurança da Informação e consequentemente provocar um acréscimo de vulnerabilidade (LIGINLAL et al., 2009). O mesmo autor coloca que a vulnerabilidade também ocorre por erro humano devido à sobrecarga de trabalho ou até mesmo por falta de atenção. Outra maneira de quebra de privacidade ou confidencialidade, conforme escrevem Goldim e Francisconi (2004) são os comentários a respeito das informações dos pacientes, feitos pelos profissionais de saúde, em qualquer ambiente hospitalar e muitas vezes inapropriado, tais como elevadores, refeitórios e corredores, pois nestes lugares podem ter a presença de pessoas estranhas e que não estejam ligadas ao atendimento do paciente e ouçam a conversa obtendo assim informações inapropriadas a respeito da saúde e tratamento do paciente.

Com a intenção de evitar esse tipo de situação, os profissionais de saúde possuem documentos regulatórios a fim de tratar de aspectos éticos nas práticas profissionais. Um exemplo é o Código de Ética Médica, Código de ética de Enfermagem, entre outros. A criação destes documentos tem a finalidade de fornecer diretrizes para a atuação profissional e uma delas é o sigilo, que segundo Massad et al. (2003) o profissional de saúde é responsável pela integridade e pela guarda da informação na qual tem acesso ao registrar, manipular, digitar, armazenar ou processar as informações.

Para Motta (2003), todos os profissionais com acesso aos dados do paciente têm o dever de manter o sigilo e a privacidade das informações e não somente os médicos que têm o acesso direto com o paciente. Isso inclui inclusive funcionários administrativos e a equipe de

enfermagem. O vazamento de informações e a invasão da privacidade dos pacientes, para Pupulim e Sawada (2002), é uma questão de ética e que deve ser tratada com mais seriedade pelos profissionais da saúde, pois a ética para eles é a Ciência da Moral e ela por sua vez refere-se ao comportamento do indivíduo.

Documentos regulatórios

Diversos documentos contêm informações ou servem como base de consulta de profissionais de saúde a respeito de privacidade de informações. Um dos documentos muito utilizado, principalmente nos Estados Unidos é a HIPAA (*health insurance portability and accountability act*), na qual o principal objetivo é a proteção dos dados de saúde e também da utilização abusiva das informações sobre a saúde do paciente. As informações médicas do paciente devem estar contidas em tecnologias a fim de protegê-las.

As informações que devem ser protegidas, de acordo com o documento, são todas aquelas relacionadas ao atendimento e aos medicamentos, como notas de visitas dos médicos, resultados e diagnósticos médicos e informações sobre a saúde. Além da proteção dos registros informatizados ela recomenda a proteção da comunicação oral e também a troca de informação por computador e armazenamento eletrônico.

O governo dos Estados Unidos, segundo Baumer (2000), padronizou os regulamentos que tratam do controle e registro de informações médicas, devido à preocupação da proteção da informação pessoal e isso aconteceu, devido a aprovação da HIPAA.

No Brasil, a agência a Agência Nacional de Saúde Suplementar (ANS), foi criada através da Lei 9.961 de janeiro de 2000, com a atribuição de regulamentar o setor de saúde. Segundo o próprio site da Instituição a finalidade institucional é promover a defesa do interesse público na assistência suplementar à saúde.

O relacionamento entre os Hospitais ou instituições de saúde e as operadoras de planos de saúde, ocorre constantemente através do intercâmbio de informações, por isso a ANS criou uma norma em nível nacional intitulada TISS (Troca de Informação em Saúde Suplementar), com a intenção de que a integração ocorra de uma maneira padronizada.

O padrão TISS teve como base além de algumas normas internacionais e nacionais a estrutura da HIPAA, tornando-se uma referência (MENDES, 2009). Os padrões utilizados em outros países foram aplicados gerando categorias únicas da área de informática em saúde, utilizadas para a troca de informações entre os prestadores de serviço e hospitais. Esses padrões criados são os padrões de comunicação, padrões de vocabulário, padrões de nomes de procedimentos médicos, padrões de conteúdo e estrutura e padrões de Privacidade.

Para auxiliar na tarefa, os sistemas devem adotar mecanismos de segurança. A certificação digital é uma tecnologia que provê estes mecanismos (CAMPARA et al., 2013). Segundo o Instituto Nacional de Tecnologia da Informação (ITI), o certificado digital é um documento eletrônico com a identificação de uma pessoa ou organização, no qual contêm além de outros dados, o nome e um número exclusivo chamado de chave pública, com a finalidade de validar a assinatura em documentos eletrônicos. No ambiente hospitalar, significa que o profissional pode assinar digitalmente o prontuário eletrônico do paciente, não necessitando fazer a impressão do documento.

Um documento que não se pode chamar nem de normativo e nem de regulatório, mas sim de consultivo e tem grande importância para os hospitais é o Manual de Acreditação, e o processo de acreditação segundo a ONA (2014) é um processo periódico e voluntário que visa garantir a qualidade da assistência de saúde através de padrões definidos. Com isso, o hospital passa a adotar normas, rotinas, guias e descrição de processos e consequentemente contribui para a padronização da assistência e a melhoria da qualidade (ALONSO et al., 2014).

Quando acreditada, a instituição é reconhecida interna e externamente pelo padrão de qualidade alcançado, por receber uma qualificação comprovada, pois alcançou um padrão de negócios e assistência externamente reconhecido (EMIDIO, 2013). O manual da JCI (2014) complementa que a acreditação possibilita melhorar a qualidade do cuidado ao paciente por trabalhar continuamente para reduzir os riscos para os profissionais e pacientes através da garantia de um ambiente seguro.

METODOLOGIA

Esta pesquisa se caracteriza como uma pesquisa exploratória de corte transversal com abordagem descritiva, utilizando dados qualitativos. O levantamento bibliográfico foi utilizado como método para a revisão sistemática. Os critérios de inclusão definidos para a seleção foram: artigos, teses e dissertações publicados em português, considerando todos os anos de publicação. Essas referências foram buscadas no *google scholar*, com as palavras chaves: "mecanismos", "privacidade da informação" e "saúde".

Foram encontrados inicialmente 200 resultados. Considerando apenas artigos, dissertações e teses, por serem consideradas fontes de informações úteis para o objetivo proposto, foram descartados 90 resultados. Os resumos dos 110 achados restantes foram lidos e com isso foram descartados mais 50, pois os mesmos citavam apenas a importância de se ter mecanismos, mas não faziam referencia a nenhuma descrição e origem. Com a leitura dos 60 achados restantes, foi possível identificar a citação de mecanismos juntamente com a norma e regulamento no qual se encontrava. Com isso foi possível encontrar em 17 referencias a descrição de documentos regulatórios e normativos.

Através destas 17 referencias identificou-se 20 possíveis documentos regulatórios que possam ter algum mecanismo de proteção de privacidade da informação. A relação dos documentos analisados consta no Quadro 2.

Quadro 2
Documentos Regulatórios e Normativos

Código	Tipo de Documento
DE1	Norma ABNT NBR ISO/IEC 27001
DE2	TISS - Troca de Informação em Saúde Suplementar
DE3	Resolução CFM Nº 1.821
DE4	Código de Ética Médica – Brasil
DE5	Código de Ética dos Profissionais de Enfermagem
DE6	Constituição Federal
DE7	Código Civil (lei 10.406)
DE8	Código de Defesa do Consumidor (lei 8.078)
DE9	Código Penal (lei nº 2.848)
DE10	Código de Ética da IMIA para Profissionais de Informática em Saúde
DE11	Lei de Acesso à informação (lei nº 12.527)
DE12	Política Nacional de Informação e Informática em Saúde (PNIIS)
DE13	HIPAA - *Health Insurance Portability and Accountability Act*
DE14	ISO / TC 215
DE15	NBR ISO/IEC 27002
DE16	Marco Civil da internet
DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
DE18	Manual de Acreditação da ONA
DE19	Manual de Acreditação da *Joint Commission International* (JCI)
DE20	PIPEDA- "*Personal Information Protection and Electronic Documents Act*"

Fonte: Elaborado pelo autor

Esses documentos foram selecionados e analisados, pois são a base de informações que deveriam servir de roteiro no tratamento de privacidade de informação para os usuários mais comuns da área da saúde. Conforme Godoy (1995), nesse tipo de abordagem três fatores devem ser observados, que é a escolha dos documentos, o acesso a eles e a sua análise. Quanto ao acesso dos documentos, os mesmos estão disponíveis em sites de internet de cada órgão institucional ou governamental.

A pesquisa documental, de acordo com Godoy (1995), pode trazer contribuições importantes para alguns estudos, e no caso desse estudo, a importância se deu porque foi através deles que foram avaliados quais tipos de recomendações existem a respeito de privacidade de informação do paciente, caso as tenha. Porém, a sua utilização, segundo Yin (1989), deve ser muito cuidadosa e planejada para que eles sirvam para aumentar as evidências de outras fontes.

A finalidade principal dessa análise de documentos foi descobrir e selecionar quais são as boas práticas que tratam de privacidade da informação do paciente. Após a seleção dos Documentos Regulatórios e Normativos, foi realizada uma análise de todos eles na íntegra, através de uma análise de conteúdo, seguindo especialmente as recomendações de Bardin (1977), pela qual primeiramente foram agrupados os dados para facilitar e melhorar os recursos durante a análise, buscando identificar os possíveis mecanismos de proteção da privacidade. O critério utilizado para a seleção dos trechos foi o de conter alguma descrição acerca de privacidade e Segurança da Informação, mesmo que indiretamente.

Posteriormente foi realizada uma classificação e a adequação de cada um dos mecanismos por tipo, ou seja, agrupando os Mecanismos de Estrutura, os Mecanismos de Processo e os Mecanismos de Relacionamento. Também foi realizada uma classificação dos mecanismos, conforme o seu eixo de ação, ou seja, vulnerabilidade, salvaguarda, detecção, punição e conscientização, com a ajuda de *experts* na área de segurança da Informação.

ANÁLISE DOS RESULTADOS

O Quadro 3 mostra o conjunto dos Documentos Regulatórios e Normativos analisados, apresentando a sua data de criação, os seus principais objetivos e a quem se aplica.

Quadro 3
Identificação dos Documentos Regulatórios e Normativos

Cód	Data de criação	A quem se aplica	Objetivos
DE1	10/2005	Todos os tipos de organizações	Específica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes
DE2	10/2005	Operadoras de planos privados de assistência à saúde e os prestadores de serviços	O principal objetivo do padrão TISS é estimular a adoção de normas nacionais de informação, a terminologia única e identificadores unívocos, a fim de permitir a interoperabilidade entre diferentes Sistemas de Informação
DE3	07/2007	Médicos, hospitais e empresas desenvolvedoras de sistemas	Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes
DE4	01/1988	Profissionais médicos	Contém as normas éticas que devem ser seguidas pelos médicos no exercício da profissão, independentemente da função ou cargo que ocupem
DE5	02/2007	Profissionais de enfermagem	Descreve os princípios, direitos, responsabilidades, deveres e proibições pertinentes à conduta ética dos Profissionais de Enfermagem
DE6	10/1988	Todos os cidadãos	Assegurar o exercício dos direitos sociais e individuais, a

Cód	Data de criação	A quem se aplica	Objetivos
		Brasileiros	liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça
DE7	01/2002	Todos os cidadãos Brasileiros	A consolidação de assuntos e negócios mais comuns, vinculados à esfera das relações jurídicas privadas
DE8	09/1990	Todos os cidadãos Brasileiros	Apresentar um conjunto de normas que visam a proteção aos direitos do consumidor
DE9	12/1940	Todos os cidadãos Brasileiros	O objetivo é penalizar as condutas ilícitas
DE10	10/2002	Profissionais de Informática em Saúde	Prover condutas éticas para os profissionais de TI em saúde e fornecer um conjunto de princípios
DE11	11/2011	Todos os órgãos públicos ou instituições particulares que recebem recursos financeiros públicos	Mostra os procedimentos a serem observados pelos órgãos Públicos, com a finalidade de garantir o acesso às informações
DE12	04/2013	Usuários do sistema SUS e população em geral	Promover o uso inovador, criativo e transformador da Tecnologia da Informação contribuindo para a melhoria da atenção à saúde da população. Também visa uma melhor governança no uso da informação em saúde e dos recursos de informática, Integrando-se ao conceito de Governo Eletrônico
DE13	08/1996	Planos de saúde e Prestador de cuidados de saúde dos EUA	Descrever formas de proteção contra a utilização abusiva de informações sobre a saúde do Paciente e a proteção dos dados de saúde do Paciente
DE14	1998	Todos os tipos de instituições de saúde e profissionais da saúde	Padronizar a informação na área da saúde; Garantir a compatibilidade de dados para fins de análise estatística, reduzindo redundâncias e duplicação de esforços
DE15	07/2007	Todas as empresas	Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de Segurança da Informação em uma organização
DE16	04/2014	Todos os usuários de internet e provedores	Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.
DE17	08/2001	Todos os Cidadãos Brasileiros	O objetivo é viabilizar a emissão de certificados digitais para identificação virtual do cidadão
DE18	1998	Hospitais que desejam buscar acreditação	Dispõe um conjunto de processos, estruturas e entidades com a finalidade de fomentar e viabilizar a acreditação
DE19	1998	Hospitais que desejam buscar acreditação	Descrever os padrões de Aceitação Hospitalar, pois contém todos os padrões, propósitos, elementos de mensuração dos padrões, políticas e procedimentos de acreditação
DE20	04/2000	Cidadãos Canadenses	Fornecer o direito de privacidade da informação

Fonte: Elaborado pelo autor

Ao término da análise dos 20 Documentos Regulatórios e Normativos, chegou-se a 37 mecanismos, conforme demonstra o Quadro 4. Em dois deles não foi possível identificar nenhum mecanismo (DE11 e DE12). Em alguns deles foi possível identificar apenas um, porém em outros foi possível a identificação de diversos mecanismos. Foi criado um código para identificar o mecanismo com as iniciais (M) e uma ordem sequencial da quantidade localizada. Também se encontra no Quadro 4 o nome, a justificativa e na última coluna estão dispostos os documentos nos quais foram encontrados os mecanismos.

O comitê da ISO/TC 215 (DE14) foi o documento com o maior número de mecanismos identificados, com 18 no total, logo em seguida aparecem a HIPAA (DE13) e a NBR ISO/IEC 27002 (DE15) com 17 mecanismos em cada um deles. No Manual de Acreditação da *Joint Commission International* (JCI) (DE19) tiveram 15 mecanismos localizados.

Mesmo não sendo possível a análise na íntegra (em virtude dos custos de aquisição), mas sim através dos resumos dos 28 documentos contidos na ISO/TC 215 (DE14), ele foi o que apresentou o maior número de mecanismos. Esse fato o faz ser um dos documentos de maior importância quando se trata de Segurança da Informação e privacidade na saúde.

Dos cinco Documentos Regulatórios e Normativos mais citados, três deles são específicos da Saúde, ou seja, a HIPAA, o manual de acreditação da JCI e considerando que foram selecionados somente os regulamentos dedicados a saúde, a ISO/TC 215.

Exceto os cinco documentos mais citados (DE14, DE13, DE15, DE19 e DE20) e também o Manual de Acreditação da ONA (DE18), com nove mecanismos, o restante deles tiverem individualmente um número pequeno de mecanismos localizados, por serem documentos muito específicos na grande maioria dos casos, como por exemplo, o Código de Ética Médica (DE4).

Quadro 4
Mecanismos encontrados nas análises dos Documentos Regulatórios e Normativos

Cód	Mecanismos	Justificativa/Objetivo	Documentos
M1	Implantar e manter um Sistema de Gestão da Segurança da Informação	Para garantir a permanência e cumprimento das políticas	DE1 – DE13 – DE14 - DE15 -DE19 – DE20
M2	Ter uma pessoa responsável pela Política de Segurança da Informação	Para garantir a permanência e cumprimento das políticas	DE13 – DE14- DE18 – DE19 – DE20
M3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	Para garantir que somente a pessoa autorizada tenha acesso à informação	DE2 –DE10 – DE13 – DE14 - DE18 – DE19 -
M4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	Para dificultar a quebra de senha e acessos indevidos	DE2
M5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	Garantir a autenticidade da informação	DE2 – DE3 – DE14 - DE17- DE18
M6	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED	Para facilitar a recuperação das informações	DE3
M7	Possuir uma Comissão de Revisão de Prontuários	Para melhorar os processos de segurança.	DE3
M8	Instruir o Médico e Enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	Evitar o vazamento da informação	DE4 – DE5 – DE9
M9	Prevenir para que Médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	Evitar o vazamento da informação	DE13
M10	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	Para evitar a divulgação de informações	DE3 - DE4 - DE5- DE6 DE7- DE9 – DE13 - DE15
M11	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	No sentido também da ética	DE3 – DE4 – DE5 - DE13 – DE14 -DE15 – DE18 – DE19
M12	Instalar Antivírus,VPN e *firewall*	Para evitar invasão por pessoas não autorizadas, sejam elas internas ou externas	DE2 - DE9 -DE13 – DE14 - DE15 - DE19 - DE20
M13	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	Para se evitar muitos acessos, por muitas pessoas, aumentando assim o risco de vazamento de informação	DE10 – DE13 – DE14 - DE15 – DE19
M14	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	Para garantir os serviços	DE1 -DE2 - DE10 – DE14 -DE15 – DE16 – DE19 –DE20

Cód	Mecanismos	Justificativa/Objetivo	Documentos
M15	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura	Para garantir os serviços	DE14 -DE18 – DE19
M16	Coletar somente dados relevantes dos clientes/pacientes	Para diminuir a possibilidade de vazamento da informação	DE10 – DE20
M17	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	Evitar muitos acessos à informação	DE10 – DE14 -DE19
M18	Evitar posicionar computadores próximos a corredores	Evita-se o acesso indevido	DE13
M19	Impor sanções adequadas para os que violam as políticas de privacidade	Impor punições para que diminua as ações	DE4 – DE5 – DE7 – DE – DE9 - DE13
M20	Penalidade com multa em dinheiro	Para evitar a ocorrência	DE13
M21	Ter um plano de recuperação ou contingência para desastres com informações	Caso tenha alguma intercorrência	DE13 – DE14 - DE15 - DE19 – DE20
M22	Ter um *backup* estruturado das informações	Para recuperar o dado caso seja perdido	DE13 – DE15 – DE18 - DE19 – DE20
M23	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede	Evitando a propagação de algum vírus ou espionagem	DE13 – DE20
M24	Ter um *software* de HIS – adequado e de boa qualidade	Para o cadastro e gerenciamento dos dados	DE14
M25	Criptografar o tráfego externo de informações	Dificulta a coleta indevida de dados	DE2 -DE13 – DE15
M26	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do Paciente	Caso seja necessário a verificação futura	DE9 -DE13 – DE14 - DE19
M27	Criar e divulgar aos colaboradores uma política de privacidade	Para que todos tenham conhecimento das regras	DE13 – DE14 -DE15 – DE18 - DE19 – DE20
M28	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa	Verificam-se maus comportamentos anteriores	DE15
M29	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo	Evita-se a coleta indevida de dados	DE15
M30	Definir regras para transmissão externa de informações para terceiros	Evita-se a coleta indevida de dados	DE14 -DE15 –DE19
M31	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação	A fim de detectar acessos indevidos	DE14 -DE15
M32	Dividir as funções dos colaboradores nos sistemas	Para que a mesma pessoa não realize todas as operações do processo, com a intenção reduzir o risco de mau uso ou uso indevido dos sistemas	DE15
M33	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação	Caso se verifique uma alteração terá tempo hábil	DE15 – DE19
M34	Analisar regularmente a Segurança dos Sistemas de Informação	Evitar a violação de alguma lei ou contratos com terceiros	DE14 -DE15 – DE18
M35	Ter a quantidade de Profissionais dimensionados de acordo com a realidade da organização ou departamento	Para evitar sobrecarga de trabalho	DE18
M36	Disponibilizar as políticas de Segurança da Informação aos clientes	Para que os clientes tenham ciência de seus direitos	DE20
M37	Manter as informações dos clientes apenas o tempo necessário por lei	Para diminuir o risco de vazamento	DE14- DE20

Fonte: Elaborado pelo autor

Já na Lei de Acesso à informação (DE11) e na Política Nacional de Informação e Informática em Saúde (DE12) não foi possível localizar nenhum mecanismo, mesmo sendo

importantes para a área da saúde. São documentos mais voltados ao Setor público e principalmente dispondo sobre o dever e meios de divulgação das informações administrativas.

Dentre os três mecanismos que mais aparecerem dois deles são voltados a ações para os colaboradores: "Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações" (M10) e "Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho" (M11). O terceiro mecanismo que mais apareceu, está relacionado ao hospital, que é "Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações" (M14).

O que se observa é que vários mecanismos foram encontrados em vários documentos, exceto 12 deles que foram citados em apenas um documento. Com isso chega-se à conclusão de que o número de Mecanismos encontrados em relação aos Documentos Regulatórios e Normativos analisados está bem distribuído, porém o número de Documentos Regulatórios e Normativos com vários mecanismos é bem restrito.

Para melhor atender ao objetivo da pesquisa, os mecanismos foram agrupados em Mecanismos de Estrutura (Quadro 5), Mecanismos de Processo (Quadro 6) e Mecanismos de Relacionamento (Quadro 7), conforme o conceito apresentado por Wiedenhoft, Luciano e Testa (2014). Segundo Guldentops, Van Grembergen e De Haes (2004) os Mecanismos de Estrutura são responsáveis por criar regras e papéis, os Mecanismos de Processo gerenciam práticas voltadas a estratégia de TI e também tem a função de implementar os sistemas de tomadas de decisões e os Mecanismos de Relacionamento são responsáveis pelo entendimento dos objetivos entre TI e negócios.

Após a classificação pelo tipo de mecanismos, foi realizada uma classificação conforme o seu eixo de ação, ou seja, vulnerabilidade, salvaguarda, detecção, punição e conscientização, (ALBRECHTSEN E HOVDEN, 2009); (LIGINLAL et al., 2009); (BULGURCU et al., 2010); (HERATH E RAO, 2009) E (D'ARCY E HOVAV, 2009).

Quadro 5
Relação final dos Mecanismos de Estrutura para a proteção da privacidade do paciente

Mecanismos de Estrutura (Código/Nome/Quantidade de citações)		Eixo de Ação	Requisito
M1	Implantar e manter um Sistema de Gestão da Segurança da Informação – 6	Salvaguarda	Confidencialidade
M2	Ter uma pessoa responsável pela Política de Segurança da Informação - 5	Salvaguarda	Confidencialidade
M6	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED - 1	Vulnerabilidade	Disponibilidade
M7	Possuir uma Comissão de Revisão de Prontuários - 1	Salvaguarda	Conformidade
M12	Instalar Antivírus,VPN e *firewall - 7*	Salvaguarda	Confidencialidade
M14	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações - 8	Salvaguarda	Disponibilidade
M23	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede - 2	Salvaguarda	Confidencialidade
M35	Ter a quantidade de Profissionais dimensionados de acordo com a realidade da organização ou departamento - 1	Salvaguarda	Disponibilidade

Fonte: Adaptado de ALBRECHTSEN e HOVDEN (2009); GULDENTOPS, VAN-GREMBERGEN e DE HAES (2004); LUCIANO e KLEIN (2014).

No Quadro 6, constam os mecanismos de processo e estão listados por uma ordem sequencial do código.

Quadro 6
Relação final dos Mecanismos de Processo para a proteção da privacidade do paciente

Mecanismos de Processo (Código/Nome/Quantidade de citações)		Eixo de Ação	Requisito
M3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices* -6	Vulnerabilidade	Confiabilidade
M4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas - 1	Salvaguarda	Confidencialidade
M5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos - 5	Salvaguarda	Confiabilidade
M11	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho - 8	Conscientização	Confidencialidade
M13	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes - 5	Salvaguarda	Confidencialidade
M15	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura - 3	Salvaguarda	Disponibilidade
M16	Coletar somente dados relevantes dos clientes/pacientes - 2	Salvaguarda	Integridade
M17	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas - 3	Salvaguarda	Confidencialidade
M18	Evitar posicionar computadores próximos a corredores - 1	Salvaguarda	Confidencialidade
M19	Impor sanções adequadas para os que violam as políticas de privacidade - 6	Punição	Conformidade
M20	Penalidade com multa em dinheiro - 1	Punição	Conformidade
M21	Ter um plano de recuperação ou contingência para desastres com informações- 5	Salvaguarda	Disponibilidade
M22	Ter um *backup* estruturado das informações - 5	Salvaguarda	Disponibilidade
M24	Ter um *software* de HIS – adequado e de boa qualidade - 1	Salvaguarda	Confidencialidade
M25	Criptografar o tráfego externo de informações - 3	Salvaguarda	Autenticidade
M26	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do Paciente - 1	Salvaguarda	Conformidade
M28	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa - 1	Salvaguarda	Integridade
M29	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo - 1	Salvaguarda	Confidencialidade
M30	Definir regras para transmissão externa de informações para terceiros – 3	Salvaguarda	Integridade
M31	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação - 2	Salvaguarda	Conformidade
M32	Dividir as funções dos colaboradores nos sistemas - 1	Conscientização	Integridade
M34	Analisar regularmente a Segurança dos Sistemas de Informação - 3	Salvaguarda	Confidencialidade

Fonte: Adaptado de ALBRECHTSEN e HOVDEN (2009); GULDENTOPS, VAN-GREMBERGEN e DE HAES (2004); LUCIANO e KLEIN (2014).

No Quadro 7, constam os mecanismos de relacionamento e estão listados por uma ordem sequencial do código.

Quadro 7.
Relação final dos Mecanismos de Relacionamento para a proteção da privacidade do paciente

	Mecanismos de Relacionamento (Código/Nome/Quantidade de citações)	Eixo de Ação	Requisito
M8	Instruir o Médico e Enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente - 3	Salvaguarda	Conformidade
M9	Prevenir para que Médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas - 1	Conscientização	Conformidade
M10	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações- 8	Conscientização	Conformidade
M27	Criar e divulgar aos colaboradores uma política de privacidade - 6	Conscientização	Conformidade

	Mecanismos de Relacionamento (Código/Nome/Quantidade de citações)	Eixo de Ação	Requisito
M33	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação - 2	Conscientização	Integridade
M36	Disponibilizar as políticas de Segurança da Informação aos clientes - 1	Salvaguarda	Integridade
M37	Manter as informações dos clientes apenas o tempo necessário por lei - 2	Salvaguarda	Disponibilidade

Fonte: Adaptado de ALBRECHTSEN e HOVDEN (2009); GULDENTOPS, VAN-GREMBERGEN e DE HAES (2004); LUCIANO e KLEIN (2014).

A separação dos três quadros finais foi realizada para facilitar a visualização e entendimento, mostrando a característica de cada mecanismo detalhadamente. A Tabela 1 apresenta um resumo do resultado, mostrando o tipo de mecanismo em relação ao Eixo de Ação.

Tabela 1:
Tipo de Mecanismo x Eixo de Ação

Eixo de Ação	Estrutura	Processo	Relacionamento	TOTAL
Vulnerabilidade	1	1	0	2
Salvaguarda	7	17	3	27
Detecção	0	0	0	0
Punição	0	2	0	2
Conscientização	0	2	4	6
TOTAL	8	22	7	37

Fonte**:** Elaborado pelo autor

O que se apresenta é que a grande maioria dos mecanismos estão classificados em mecanismos de processos e grande parte deles no eixo de salvaguarda, tendo a conscientização, que segundo (BRAGANÇA et al., 2010) é uma característica importante para se ter um bom êxito na proteção da informação, um número bastante baixo em relação ao total de mecanismos, o que é bastante preocupante.

Considerando o item conscientização do Eixo de Ação, somente seis mecanismos foram encontrados, de um total de 37 mecanismos. Do total de mecanismos classificados como conscientização dois deles estão classificados como mecanismos de Processos e quatro deles como de Relacionamento. O que é muito baixo, pois, uma das grandes preocupações é exatamente as atitudes e as influências comportamentais do ser humano.

Dois aspectos podem influenciar o comportamento de uma pessoa. O primeiro é no que a pessoa acredita: suas convicções, seus princípios e valores, e o segundo é o meio ambiente: tais como os valores organizacionais, opinião dos colegas e a cultura organizacional (LUCIANO; MAÇADA; MAHMOOD, 2010). Esses fatores são melhorados levando em consideração a conscientização dos colaboradores, buscando sempre o bom comportamento.

A intenção no comportamento pode influenciar a Segurança da Informação, uma vez que a informação é um ativo, como qualquer outro ativo importante para procedimentos de saúde, e tem um valor para o meio e consequentemente necessita ser protegida de forma adequada (ABRAHÃO, 2003).

O incentivo à conscientização por parte dos documentos analisados, ou seja, a apresentação desses mecanismos mais claros, se faz importante, pois, segundo Klein (2014 p.91) "as orientações de conscientização sobre Segurança da Informação precisam ser elaboradas para destacar a Severidade e a Suscetibilidade da Ameaça e devem se concentrar em educar os usuários sobre a possibilidade e os danos das ameaças, possibilitando que o usuário entenda a necessidade de segurança, o seu papel e a sua responsabilidade na proteção de dados organizacionais".

CONCLUSÃO

O artigo traz como resultado principal a implementação do conhecimento com a descrição de mecanismos de privacidade da informação em ambientes hospitalares, assim como a descrição dos documentos regulatórios e normativos que contém esses mecanismos. O resultado da revisão sistemática pode fornecer uma base de documentos para administradores hospitalares e também pesquisadores que embasem práticas que protejam a informações dos pacientes.

Mesmo que se tenha uma grande preocupação com a privacidade da Informação na área da saúde, o Brasil não conta com um documento que trata especificamente do assunto, nem mesmo uma lei para reger e orientar os usuários. O que se tem são trechos de documentos indicando mecanismos para a proteção das informações dos pacientes, conforme localizados através do artigo.

Como limitação do estudo está a impossibilidade de uma pesquisa mais profunda nos documentos da ISO/TC 215 devido ao alto custo assim como a classificação somente com 2 *experts* em segurança. E como pesquisas futuras propõe-se realizar uma survey para fazer a classificação dos mecanismos, estudar outros fatores de requisitos de segurança para pontuar a situação atual dos mecanismos propostos nos documentos.

REFERÊNCIAS

ABRAHÃO, M. S. A Segurança da Informação Digital na Saúde. Sociedade Beneficente Israelita Brasileira, 2003. Disponível em: <http://www.einstein.br/biblioteca/artigos/131%20132.pdf>. Acesso em: 30 Jun. 2014.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. (jan/fev 2005).Privacy and Rationality in Individual decision making. IEEE Security & Privacy. IEEE Computer Society. v.3, n.1, p. 26-33.

ALBRECHTSEN, E.; HOVDEN, J. (2009). The information security digital divide between information security managers and users. **Computers & Security**, v. 28, n. 6, p. 476-490.

ALONSO, L. B. N.; DROVAL, C.; FERNEDA, E.; EMÍDIO, L..(jul./dez. 2014). Acreditação Hospitalar e a Gestão da Qualidade dos Processos Assistenciais. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n. 2, p. 34-49.

ANS - AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. (2013). PADRÃO TISS. Segurança & privacidade, Novembro.

BARDIN, L. (1977). Análise de conteúdo. Lisboa: Ed. 70.

BAUMER, D.; EARP, J.; PAYTON, F. (2000). **Privacy of Medical Records: IT implications of HIPAA**, New York: ACM Press.

BOSS, S. R.; KIRSCH, L. J.; ANGERMEIER I.; Shingler R. A.; WAYNE R. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. **European Journal of Information Systems**, 18,151–164.

BRAGANÇA, C. E. B. A; LUCIANO, E. M.; TESTA, M. G..(2010). Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise

exploratória da privacidade percebida pelos profissionais. **EnANPAD**. Rio de Janeiro – 25 a 29 de setembro.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I.. (2010). Information Security Policy: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly** Vol. 34 No. 3 pp. 523-548/Sepember.

CAMPARA, M.; ALKIMIN, R. A.; MESQUITA, J. M. C; MUYLDER, C. F.; DIAS, A. T.; LA FALCE, J. (2013). Implantação do Prontuário Eletrônico de Paciente**, Revista de Administração Hospitala**r, v.10, n.3, pp. 61-74, setembro/dezembro.

CONSELHO FEDERAL DE MEDICINA. (1988). Código de Ética Médica. Diário Oficial da União; Poder Executivo, Brasília, DF, de 26 jan. Seção 1, p. 1574-7.

CONSELHO FEDERAL DE MEDICINA. **(**2007). **RESOLUÇÃO CFM Nº 1.821, DE 11 DE JULHO DE 2007**. Diário Oficial da União; Poder Executivo, Brasília, DF, 23 nov. Seção I, p. 252

D'ARCY, J.; HOVAV, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. **Journal of Business Ethics**, v. 89, p. 59-71.

EMÍDIO, L.F.; ALONSO, L.B.N.; FERNEDA, E.; HEDLER, H.C.. (2013). Acreditação Hospitalar: Estudos de Caso no Brasil. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 3, n. 1, p. 98-113, jan./jun.

FERREIRA, F. N. F.; ARAÚJO, M.T. (2008). **"Políticas de Segurança da Informação - Guia prático para elaboração e implementação"**. Rio de Janeiro: Ciência Moderna.

GAERTNER, A.; SILVA, H. P. (2005). Privacidade da Informação na Internet: Ausência de Normalização, Proceedings. **CINFORM - Encontro Nacional de Ciência da Informação VI**, Bahia.

GODOY A. S. (1995). Pesquisa Qualitativa: Tipos Fundamentais. **RAE** • v. 35 • n. 3 • Mai./Jun., São Paulo, Brasil.

GOLDIM, J. R.; FRANCISCONI, X. (2004). **Bioética Clínica.** Disponível em: < http://www.pucrs.br/bioetica/cont/carlos/bioeticaclinica.pdf> Acesso em: 25 Jun. 2014.

GULDENTOPS, E., VAN-GREMBERGEN, W. e DE HAES, S. (2004). Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool. **Information Systems Control Journal**, v6, p.32-35.

HENDERSON S.C., SNYDER C.A. (1999). Personal information privacy: implications for MIS managers, **Information & Management**. 36(4), p. 213–220.

HERATH, Tejaswini; RAO, H. Raghav. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations**. European Journal of Information Systems**, v. 18, n. 2, p. 106-125.

HIPAA. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF (1996) - U.S. Department of Health & Human Services, AUG. 21.

ICP Brasil. (2001). Medida Provisória Nº 2.200 de 28 de junho.

IMIA - Código de Ética da IMIA para Profissionais de Informática em Saúde. Disponível em< http://www.imia-medinfo.org/new2/>. Acesso em: 10 Dez. 2014.

ISO/IEC 27001. (2013). Information technology -- Security techniques -- Information security management systems – Requirements.

ISO/IEC 27002. (2013). Information technology -- Security techniques -- Code of practice for information security controls.

ITI - Instituto Nacional de Tecnologia da Informação. Disponível em < www.iti.gov.br>. Acesso em: 27 Jun. 2014.

JCI - *Joint Commission International Accreditation – Standards for Hospital* – Disponível em: http://www.jointcommissioninternational.org/: Acesso em: 10 dez. 2014

KLEIN, R. H.. (2014). Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à Segurança da Informação. 24/03/214. 100 f. Dissertação (Mestrado em Administração) - Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul.

LEINO-KILPI H., et.al. (2001). Privacy: a review of the literature. **International Journal of Nursing Studies** 38, 663–671.

LIGINLAL, D.; SIM, I.; KHANSA, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. **Computers & Security**.v.28, p.215-228.

LUCIANO, E. M.; MAÇADA, A. C. G.; MAHMOOD, M. A. (2010). " The influence of human factors on vulnerability to information security breaches". **AMCIS 2010 Proceedings. Paper,** 351.

LUCIANO, E. M.; BRAGANÇA, C. E. B. de A.; TESTA, M. G. (2011). Privacidade de informações de pacientes de instituições de saúde: a percepção de profissionais da área de saúde. **Reuna** (Belo Horizonte), v. 16, p. 89-102.

LUCIANO, E. M.; KLEIN, R. H. – In. PRADO, E.P.V.; SOUZA C.A. (Orgs). (2014). Fundamentos de Sistemas de Informação, 1 ed. Rio de Janeiro: Elsevier, cap. 6, p. 93-110.

MASSAD, E., MARIN, H.F., AZEVEDO, R. S. (2003). O Prontuário do Paciente na Assistência, Informação e Conhecimento Médico. São Paulo. USP.

MENDES, S. F. et al. (2009).Uma análise da implantação do padrão de troca de informação em saúde suplementar no Brasil. **J. Health Inform**. Out-Dez; 1(2): 61-7

MOTTA, G. H. M. B. (2003). Um Modelo de Autorização Contextual para o Controle de Acesso ao Prontuário Eletrônico do Paciente em Ambientes Abertos e Distribuídos.05/02/2004. 213 f. Tese (Escola Politécnica). USP.

NRC. (1997). National Research Council. For the Record: Protecting Electronic Health Information.

ONA. (2014). ORGANIZAÇÃO NACIONAL DE ACREDITAÇÃO. Manual das Organizações Prestadoras de Serviço de Saúde, Brasília.

PUPULIM, J. S. L.; SAWADA, N. O. (2002). O cuidado de enfermagem e a invasão de privacidade do doente: uma questão ético-moral. **Revista Latino-americana de Enfermagem**. V. 10, 3, p. 483-488.

SÊMOLA, M. (2003). **Gestão de Segurança da Informação – uma visão executiva**. 8ª. Ed, Rio de Janeiro: Elsevier.

SIPONEN, M. (2000). A conceptual foundation for organizational information security awareness, **Information Management & Computer Security**, 8, 1, 31-41.

SMITH, M. (1996).Data protection, health care and the new European directive. **British Medical Journal** 312, 197–198.

VANCE, A.; SIPONEN, M.; PAHNILA, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. **Information & Management**.

WIEDENHOFT, G. ; LUCIANO, E. M. ; TESTA, M. G. (2014). A Indicators Based Approach to Measure Informati on Technol ogy Governance Effectiveness: A Study with Brazilian Professionals. In:22nd European Conference on Information Systems, 2014, TelAviv. **Procedings of the 22nd European Conference on Information Systems**.

YIN, R. K .(1989). Case Study Research - Design and Methods. **Sage Publications Inc**., USA.