PRIVACIDADE DE INFORMAÇÕES DE PACIENTES DE INSTITUIÇÕES DE SAÚDE: A PERCEPÇÃO DE PROFISSIONAIS DA ÁREA DE SAÚDE

PRIVACY OF INFORMATION FOR PATIENTS OF HEALTH INSTITUTIONS: THE PERCEPTION OF HEALTH PROFESSIONALS

Edimara Mezzomo Luciano
Pontifícia Universidade Católica do Rio Grande do Sul

Doutorado em Administração pela Universidade Federal do Rio Grande de Sul -UFRS
Endereço: Av. Ipiranga, 6681, Prédio 50, sala 1105 – CEP 90619-900 - Porto Alegre - RS
Telefone: (51) 33203515 Ramal: 4082 Fax: (51) 33203524
Email: eluciano@pucrs.br
Lattes: http://lattes.cnpq.br/2607532326321244

Carlos Eduardo Barbosa de Azevedo Bragança
Pontifícia Universidade Católica do Rio Grande do Sul

Mestre em Administração pela Pontifícia Universidade Católica do Rio Grande do Sul
Endereço: Av. Ipiranga, 6681, Prédio 50, sala 1105 – CEP 90619-900 - Porto Alegre - RS
Telefone: (51) 33203515 Ramal: 4082 Fax: (51) 33203524
Email: braganca.ce@gmail.com
Lattes: http://lattes.cnpq.br/7158974470591632

Mauricio Gregianin Testa
Pontifícia Universidade Católica do Rio Grande do Sul

Doutor em Administração pela Universidade Federal do Rio Grande do Sul - UFRS
Endereço: Av. Ipiranga, 6681, Prédio 15, Sala 212, Partenon. CEP 90619-900 - Porto Alegre, RS
Telefone: (51) 33538326
Email: mauricio.testa@pucrs.br
Lattes: http://lattes.cnpq.br/2578621900901541

Data de submissão: 11 Abr. 2011. **Data de aprovação**: 30 Ago. 2011. **Sistema de avaliação**: *Double blind review*. Centro Universitário UNA. Prof. Dr. Mário Teixeira Reis Neto, Profª. Dra. Wanyr Romero Ferreira

Agência de Financiamento: CNPq

Resumo

As organizações têm aumentado a utilização de Sistemas de Informação e, em consequência, a quantidade de dados sobre clientes registrada nesses sistemas, o que leva à preocupação com a Segurança da Informação. No campo de informações sobre pacientes, a privacidade das informações adquire especial relevância, já que o vazamento de informações desse tipo pode ser catastrófico para os usuários dos serviços de saúde e seus familiares. O tema deste estudo é a segurança da informação, mais especificamente sobre privacidade das informações armazenadas em SI, e o foco é na privacidade percebida por profissionais de saúde. O objetivo é compreender a percepção dos profissionais de saúde com relação à privacidade das informações de pacientes no âmbito da Segurança da Informação. Este trabalho é de caráter exploratório, e a coleta de dados ocorreu por meio de entrevistas semiestruturadas com sete profissionais da área da saúde que têm relação direta com aspectos relacionados à segurança da informação ligados a quatro diferentes instituições hospitalares e de ensino do estado do Rio Grande do Sul. O trabalho faz parte de uma pesquisa mais ampla, que investiga a privacidade percebida por todos os atores

envolvidos no manuseio dessas informações. Os resultados mostram deficiências significativas acerca do encaminhamento dado para o problema de segurança e privacidade em informações de saúde, em especial na utilização de políticas sobre informações privadas, as responsabilidades dos profissionais envolvidos, a capacitação desses profissionais e os desafios relacionados à privacidade das informações de saúde.

Palavras-chave: Segurança das informações. Privacidade. Informação dos pacientes.

Abstract

Organizations have increased the use of information systems and, consequently, the amount of data about clients registered in these systems, resulting in concerns about information security. In the field of patient information, privacy takes on special relevance, because the leak of these informations could be catastrophic for users of health services and their families. The subject of this study is the information security, specifically about privacy of information stored in SI, and focused on perceived privacy by health professionals. The objective is to understand the perception of health professionals regarding the privacy of patient information under the Information Security. This study is exploratory, and data collection was through semi-structured interviews with seven healthcare professionals who have direct relationship with aspects related to information security. The professionals are linked to four different hospitals of Rio Grande do Sul state. The study is part of a larger study, which investigates the privacy perceived by all actors involved in handling this information. The results show significant shortcomings about security and privacy of health information, particularly on the use of private information, responsibilities of professionals involved, and challenges related to privacy on health information.

Key-words: Information Security, privacy, patients' informations

1 – Introdução

As organizações têm, com o passar do tempo, aumentado a utilização de Sistemas de Informação (SI) e, em consequência, a quantidade de dados sobre clientes registrada nesses sistemas. Isso se deve, segundo Ng, Kankanhalli e Xu (2008), à confiança atual em sistemas de informação para a transmissão, processamento e armazenamento da informação. O mesmo ocorre em organizações da área de saúde, as quais têm feito uso intensivo de Tecnologia da Informação (TI) como apoio às suas atividades. Contudo a adoção e utilização de TI precisam ser cuidadosamente acompanhadas de mecanismos que garantam a segurança dessas informações, uma vez que surgem em paralelo novas ameaças e riscos. A preocupação com a segurança e proteção dessas informações adquire caráter de extrema relevância (D'ARCY; HOVAV; GALLETTA, 2009).

Vários são os aspectos relacionados à segurança da informação. Afora os conceitos técnicos, existem outros aspectos que devem ser considerados, tais como privacidade, risco, vulnerabilidade e confiança. Cho (2006) cita que esses itens são necessários para que seja possível obter a efetividade dos procedimentos que visam à segurança da informação.

Gaertner e Silva (2005) afirmam que o histórico médico de um indivíduo está entre os tipos de informação que mais se deseja preservar. É fato que o vazamento de informações desse tipo pode ser catastrófico para os usuários dos serviços de saúde e seus familiares, uma vez que os danos causados pelo vazamento acidental ou voluntário de dados e informações sigilosas podem ser irreversíveis. Acquisti e Grossklags (2007) ressaltam que nem sempre sabemos quando, onde e como o todo ou parte de informações pessoais, que deveriam ser privadas, estão sendo utilizadas.

A despeito da necessidade em se manter a privacidade no armazenamento e manipulação desses dados, existe a necessidade de que eles sejam compartilhados, pela impossibilidade em se efetuar um tratamento sem acesso aos mesmos. A informação deve ser protegida e

processos de segurança devem ser gerenciados, independentemente da forma como essa informação é armazenada, transmitida ou acessada (MOREIRA, 2001), e acessível para as pessoas certas, na devida quantidade (nunca a mais do que cada usuário necessita para sua tomada de decisão) e disponível sempre que necessário.

Este trabalho tem como tema a segurança da informação, mais especificamente sobre privacidade das informações armazenadas em SI. A privacidade, no contexto de organizações de saúde, é relacionada ao sigilo das informações contidas em prontuários médicos e ao comportamento seguro dos profissionais que diariamente acessam essas informações. Privacidade é igual ao que falar, com quem falar e, não menos importante, onde falar, já que profissionais autorizados a ter acesso a determinadas informações podem discuti-las em ambiente inadequado, onde outras pessoas podem ouvi-los, e assim ocorreria um vazamento de informações privadas de seus pacientes. A questão de pesquisa que orientou todo o trabalho foi: qual a percepção que os profissionais de saúde, que atuam no ambiente hospitalar, têm em relação aos métodos de coleta, armazenamento, manipulação e à privacidade dos registros de seus pacientes? O objetivo estabelecido foi compreender a percepção dos profissionais de saúde com relação à privacidade das informações de pacientes no âmbito da Segurança da Informação. A justificativa para o estudo consiste na necessidade de ampliação do conhecimento sobre aspectos humanos em segurança da informação, já que os aspectos tecnológicos não conseguem sozinhos prover adequados níveis de segurança da informação (RANSBOTHAM; MITRA, 2009).Os resultados encontrados contribuiem para a compreensão de aspectos adjacentes à segurança da informação, permitindo a elaboração de políticas de segurança mais efetivas.

2- Referencial Teórico

Em que pese o risco de que informações sobre clientes vazem pela internet, há de se considerar que esta não é a única forma de quebra de privacidade. Elas podem ser voluntárias e indevidamente extraídas, através de comentários em conversas dentro da instituição hospitalar e igualmente fora dela. Acquisti e Grossklags (2003) investigaram as causas da dicotomia existente entre a intenção de comportamento e concluíram que, mesmo existindo atualmente diversas tecnologias que visam a garantir a privacidade das informações, muitas delas, aparentemente, não têm obtido êxito nesse sentido, podendo ser a divulgação por meio de profissionais (e não por meios eletrônicos) a explicação dessa divergência.

Tomando como base o tratamento interno dado às informações médicas dentro do ambiente hospitalar, pode-se ressaltar a importância da capacitação e do comportamento não somente dos profissionais de saúde, mas também dos profissionais de Tecnologia da Informação, na ética profissional em relação ao sigilo dessas informações dentro e fora do ambiente hospitalar.

A seguir, abordam-se os pilares desta pesquisa, quais sejam, segurança da informação, privacidade e estes aplicados à área da saúde.

2.1 Segurança da Informação

A informação é um dos bens mais valiosos de qualquer organização. E, como tudo que é valioso, deve ser adequadamente guardado e protegido. Dessa forma, Segurança da Informação é a proteção dos ativos informacionais de uma organização, em relação às perdas, exposição indevida ou dano (WILLIAMS, 2001). É um conceito que se aplica a toda informação armazenada, manipulada ou transmitida em uma ou entre organizações.

A Segurança da informação é alcançada a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais ou

ainda funções de software. Esses controles precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos (ABRAHÃO, 2003).

Segurança é uma expressão que procura transmitir conforto e tranquilidade a quem se beneficia da condição de estar seguro. Ela abraça políticas, procedimentos e medidas técnicas utilizadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a Sistemas de Informação. Assim, dado o destacado papel da TI para as organizações atuais, a Segurança da Informação é um elemento chave para o planejamento e gerenciamento da empresa moderna (CHANG; HO, 2006). A Segurança da Informação também é definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003). Sua principal finalidade é a de buscar proteger a informação de um conjunto de ameaças a fim de garantir a continuidade do negócio, minimizar as perdas empresariais e maximizar o retorno dos investimentos e as oportunidades de negócios (MANDARINI, 2004). Nesse contexto, a Segurança da Informação é um dos muitos requisitos que têm estado presente no dia a dia das organizações e de seus funcionários (ALBRECHTSEN, 2007).

As declarações do autor deixam clara a vinculação da Segurança da Informação com a área de gestão e mesmo o seu caráter estratégico para as organizações.

A Proteção de um ativo ou bem representa que este possui um valor para o seu proprietário (MANDARINI, 2004). Entretanto o campo da Segurança da Informação tradicionalmente tem sido direcionado para problemas técnicos e suas soluções e tem deixado a desejar na atenção aos aspectos humanos e socio-organizacionais (DHILLON; BACKHOUSE, 2001). Contudo, independente da origem do problema, tem-se que levar em conta que o alvo sempre é a informação, que não se restringe a um único ambiente físico ou sistema computacional. Ela está presente em toda a empresa e sujeita aos mais diversos tipos de riscos ou ameaças (SÊMOLA, 2003).

Outro aspecto de igual importância é a participação do usuário de sistemas na Segurança da Informação. Eles desempenham um papel ativo na atividade de prevenir incidentes indesejáveis e proteger os ativos materiais e virtuais das organizações. Os usuários podem ainda contribuir com diversas ações seguras em seu dia a dia, como, por exemplo, bloquear sua estação de trabalho ao sair, adotar uma política de senhas, com trocas frequentes, ter cuidados no uso de e-mail e internet, usar softwares licenciados e, principalmente, comunicar as falhas de segurança eventualmente detectadas (ALBRECHTSEN, 2007).

Entre os aspectos observados pela Segurança da Informação está a privacidade dos dados dos usuários. Um dos mecanismos para que esse objetivo seja alcançado é a existência de uma política de privacidade. Ela é o documento que, em teoria, informa ao usuário a maneira pela qual suas informações pessoais serão coletadas, manipuladas e armazenadas. Ela transmite como as informações serão seguradas e para que serão utilizadas. Esse assunto será abordado na seção seguinte.

2.2 Privacidade

Derivada do latim *privatus*, que significa aquilo que está fora da alçada do Estado, sendo pertencente à própria pessoa, ao próprio indivíduo, a privacidade pode também ser definida como um conceito que se caracteriza pela capacidade que cada indivíduo tem de proteger e gerenciar o acesso às suas informações pessoais. Em um sentido geral, Silva (2001, p. 206) diz que a privacidade pode ser entendida como o "conjunto de informações acerca do indivíduo o qual ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em quais condições, sem a isso ser legalmente sujeito". A privacidade de um indivíduo e de suas informações é um direito de cada cidadão e a ele pertence. Dessa forma, nenhuma organização deve negligenciar essa responsabilidade nem descuidar de nenhuma informação que lhe for confiada (MOREIRA, 2001; FONTES, 2006).

A discussão sobre privacidade remonta a tempos antigos. Em seus ensaios sobre ética e política, Aristóteles diz que um dos papéis da política liberal é o de garantir uma zona de

privacidade e a liberdade dos cidadãos, na qual eles possam viver sua vida de acordo com sua vontade, independente do julgamento alheio, desde que não causando mal a outros (SWANSON, 1992, p. 36). Em 1873, um estudo do juiz americano Thomas Colley, chamado de "*The Elements of Torts*", deu uma definição clássica para a palavra privacidade, como o direito de estar em paz e de ser deixado sozinho. A partir daí, diversas outras áreas do conhecimento passaram a estudar a privacidade, como, por exemplo, a sociologia, a comunicação, as chamadas ciências da saúde e, principalmente, o direito.

Quando se fala em Tecnologia da Informação, a privacidade é geralmente citada como o equilíbrio entre o risco de suprir as organizações com informações sobre as pessoas e os benefícios gerados pelo acesso do usuário a essas informações e serviços. Outra maneira de se observar a privacidade é relacioná-la com a preocupação do indivíduo em perder o controle sobre o uso e disseminação de suas informações pessoais (ROSE, 2006, p. 323). Alguns autores dizem ainda que "privacidade é a reivindicação dos indivíduos, grupos e instituições em determinar quando, como e quais informações sobre si mesmos serão transmitidas a outros" (WESTIN, 1967, P. 7; ROSE, 2006, p. 323).

Quanto menos se tem privacidade, menos controle se tem sobre a vida, sobre o destino ou ainda a respeito da utilização lícita ou ilícita de nossas informações pessoais. Dyson (1998, p. 217) cita que "a privacidade real - que é o respeito pelas pessoas e não mera ausência de dados – depende do discernimento humano e do bom senso". Ela está ligada à vigilância e à segurança. Necessário se faz, então, que o equilíbrio entre privacidade, segurança e controle seja alcançado, de forma a garantir a preservação dos direitos tanto coletivos quanto individuais.

2.3 Segurança da Informação e Privacidade na área da saúde

Atualmente é reconhecida e de consenso entre os gestores de instituições a importância das informações em saúde para o gerenciamento da qualidade dos serviços médicos (OLIVEIRA; JANSSEN, 2007). Somando-se a isso o fato de que cada vez mais se tem uma maior quantidade de informações armazenadas sobre o histórico de saúde dos pacientes. Nesse contexto, a privacidade das informações médicas de um paciente é um direito deste da mesma forma em que é igualmente uma obrigação do profissional de saúde que o atende. E esse direito não se extingue com a morte da pessoa. A Declaração de Genebra, de 1924, diz que "os segredos confiados ao profissional de saúde deverão ser respeitados mesmo após a morte do paciente". Dessa forma, o dever de confidencialidade que todos os profissionais de saúde devem observar mantém-se mesmo após a morte do paciente (GOLDIN; FRANCISCONI, 2004).

Com as novas tecnologias e ferramentas, as informações dos pacientes podem estar disponíveis a qualquer tempo, em qualquer lugar e a qualquer um, desde que cada um desses *locus* estejam devidamente identificados e autorizados ao acesso e manipulação dessas informações. As brechas existentes na área de segurança desses dados podem causar danos irreversíveis à reputação dessas instituições, bem como às vidas dos usuários envolvidos. Tais falhas podem acontecer não somente nos sistemas, mas também entre os profissionais envolvidos. Comentários a respeito de dados de pacientes, conversas informais em ambientes públicos, mesmo que sejam dentro da própria instituição, podem resultar em rupturas no processo de segurança desses dados. Corroborando essa preocupação, Goldin e Francisconi (2004) citam que "as informações que os pacientes fornecem, quando de seu atendimento em um hospital, posto de saúde ou consultório privado, assim como os resultados de exames e procedimentos realizados com finalidade diagnóstica ou terapêutica são de sua propriedade". Como exemplo, eles afirmam ainda que, em um hospital de grande porte, durante uma internação, até 75 pessoas diferentes chegam a lidar com o prontuário de um paciente.

Janczewski e Shi (2002) afirmam que o cuidado com a saúde tem se transformado com o desenvolvimento da medicina moderna. Em vista disso, os usuários e seus familiares, que antes estavam acostumados ao funcionamento tradicional de um hospital, hoje, com a

ampla utilização da TI e da internet, não estão acostumados a esse novo panorama, onde as informações sobre suas vidas e das vidas de seus entes estão disponíveis e acessíveis em qualquer lugar e a qualquer tempo. Eles podem se sentir invadidos, devassados em sua intimidade, desconfiados quanto à privacidade de sua vida, de suas informações. Nesse sentido, países como os Estados Unidos têm procurado controlar essas atividades, com a publicação de leis, entre elas o Health Insurance Portability and Accountability Act (HIPAA), promulgado como um Ato de Lei que visa a proteger toda informação pessoal disponibilizada e utilizada na prestação de serviços de saúde. De acordo com Baumer, Earp e Payton (2000), esse ato pode ser visto como a resposta oficial para preocupações éticas e morais de proteção da informação do indivíduo na forma da Lei nos Estados Unidos. Ele define diretivas dos direitos à privacidade e à segurança de registros de saúde. Contudo o Brasil ainda carece de legislação nesse 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, além de normas e padrões para o envio de informações de natureza econômico-financeira.

Assim, é de fundamental importância a preservação da privacidade do paciente, bem como de todas as suas informações, juntamente com o desenvolvimento de mecanismos de gestão para controle e acompanhamento do processo.

3 - Procedimentos metodológicos

Esta pesquisa é de caráter exploratório, e assim se justifica, uma vez que não foram localizados na literatura instrumentos adequados aos seus objetivos, além de permitir ao pesquisador ampliar significativamente o conhecimento sobre o tema deste estudo.

A coleta de dados ocorreu por meio de entrevistas semiestruturadas com sete profissionais da área da saúde que têm relação direta com aspectos relacionados à segurança da informação. Mesmo sendo em pequeno número, o conjunto de profissionais é de grande relevância no assunto, sendo reconhecidos como especialistas no assunto. Os profissionais estão ligados a quatro diferentes instituições hospitalares e de ensino do estado do Rio Grande do Sul, sendo que estas são referências no atendimento a pacientes.

Esses respondentes foram selecionado por possuírem conhecimento no assunto e por fazerem parte de dois grupos fundamentais ao tema: o de gestores e o de Assistência Multiprofissional à Saúde. Estes têm, em grande parte de sua atividade assistencial diária, acesso a uma maior quantidade de informações sobre os pacientes e um contato direto com eles. O objetivo das entrevistas foi investigar práticas e conceitos utilizados por profissionais de saúde e instituições hospitalares nos quesitos Segurança da Informação e Privacidade de Registros Médicos. Todas as entrevistas foram gravadas, transcritas e tiveram a sua transcrição conferida.

A análise dos dados foi feita utilizando-se a técnica de Análise de Conteúdo, com a utilização da técnica de análise categorial, que utiliza como base a decodificação de um texto em diversos elementos, também chamados de unidades de registro. Em seguida, esses elementos foram classificados e formaram agrupamentos, de acordo com o sugerido por Bardin (1977). Essas unidades foram selecionadas, segundo o critério de tema. Também é chamada de análise temática e tem a finalidade de identificar os chamados núcleos de sentido nas entrevistas transcritas.

4 - Resultados

A seguir apresenta-se a caracterização dos respondentes e a percepção destes em relação à privacidade de informações de pacientes.

4.1 Caracterização dos Entrevistados

Os entrevistados, em número de sete, têm atuações distintas dentro do escopo de tratamento multidisciplinar em que operam na área da saúde. O QUADRO 1, a seguir, mostra uma síntese de atuação e experiência de cada um dos entrevistados.

QUADRO 1 – Desafios relacionados à privacidade

Principal formação	Atuação atual	Papel	Anos de experiência	Referência neste texto
Médica	Clínica/Hospital	Gestão	30 anos	RESP1-M
Médica	Chefe da seção de prontuário	Atendimento multiprofissional	25 anos	RESP2-M
Médico	Diretor clínico	Gestão	32 anos	RESP3-M
Enfermeira	Clínica/Hospital	Atendimento multiprofissional	18 anos	RESP4-E
Psicóloga	Clínica/Hospital	Atendimento multiprofissional	15 anos	Resp5-E
Filosofia	Comitê de Bioética	Gestão	28 anos	Resp6-B
Psicologia	Clínica/Hospital	Atendimento multiprofissional	13 anos	Resp7-P

Fonte: Elaborado pelos autores com os dados da pesquisa

Todos são referência nas suas áreas pela experiência nacional e internacional, quando se fala em privacidade na área da saúde.

4.2 Análise dos resultados das entrevistas

A primeira questão abordou a opinião dos entrevistados sobre o que estes consideram privacidade na área da saúde. De maneira geral, os respondentes citaram que esta é um direito que o paciente tem de que as informações sobre a vida dele sejam respeitadas. Resp2-M ressaltou que esse conceito aplica-se a qualquer paciente, mesmo que este seja um colega de trabalho da instituição médica que está como paciente no momento, citando que é comum se relativizar a privacidade nessas situações.

A segunda pergunta abordava quais as informações dos pacientes que os respondentes consideram como as mais sigilosas. Na resposta a essa questão, não houve concordância. Alguns respondentes consideraram que todas as informações de pacientes são sigilosas. Resp3-E ressaltou que a privacidade é difícil de delimitar, pois ela muda entre pacientes, sendo a visão de cada um quais as suas informações não podem ser divulgadas. Essa é uma das dificuldades da privacidade, já que há um juízo de valor dos profissionais envolvidos que pode ser diferente daquele do paciente.

A terceira pergunta tratou dos principais desafios em se manter os registros dos pacientes seguros, e da relação desses desafios com as políticas e sistemáticas das instituições e com o comportamento dos profissionais. Resp3-M comentou que esses desafios são tecnológicos, de impedir o acesso não autorizado às informações de pacientes. Já Resp4-E comentou que o maior desafio é comportamental, de formação da ação correta dos profissionais, fato agravado pela quantidade de jovens profissionais, que ainda não têm muita noção sobre a gravidade de algumas consequências de atos ou negligências quanto ao sigilo das informações. Resp1-M citou, como desafio, tanto a melhoria de processos

manuais, evitando que um prontuário em papel fique exposto à consulta de pessoas não autorizadas, quanto a melhoria dos processos de segurança da informação para aquelas instituições que usam prontuário eletrônico. Resp5-E comentou que o formulário em papel invariavelmente gira nas mãos de muitas pessoas, inclusive alguns que não necessitariam ter acesso a esse conjunto de informações. Resp2-M ressaltou que, independente do prontuário ser em papel ou eletrônico, é de extrema importância que as organizações definam mecanismos de entendimento que motivem os profissionais a acessarem essas informações, desenvolvendo mecanismos de controle no sentido de evitar acessos não autorizados. Resp2-M ressaltou ainda que é uma questão muito mais de caráter humano e cultural do que técnico ou tecnológico, opinião compartilhada também por Resp1-M. Resp6-B também reforçou a necessidade de mudança da cultura atual, de onipotência do cuidador de saúde em relação ao paciente, já que muitos profissionais utilizam a eventual vulnerabilidade do paciente com prepotência, passando a enxergar o paciente como um objeto, que dele depende.

A questão seguinte tratou mais especificamente das políticas de acesso às informações de pacientes. O Resp5-E comentou que, embora as políticas sejam fundamentais, nem todos os profissionais vão considerá-las importantes. Resp3-M comentou que as políticas de que tem conhecimento são bastante adequadas. No entanto Resp1-M, que trabalha na mesma instituição, comentou que é preciso separar o fato dessas políticas estarem claramente redigidas e o fato de que os profissionais as sigam. Fatores culturais, de relativização das consequências e punições do não seguimento dessas políticas impediriam a efetividade dessas políticas, segundo Resp6-B. Resp2-M reforçou o desafio comportamental, até por parte do paciente, citando o fato de que hoje o paciente pode retirar o prontuário para fazer uma copia, e se corre o risco de que, ao fazer a cópia solicitada, outra cópia seja feita e com isso a privacidade rompe-se, não por erro da instituição de saúde, mas por parte do paciente. Resp2-M comenta, em resposta a outra questão, que é proibido tirar cópia do prontuário, só o médico pode fazer cópia (se precisar se defender em juízo). Um aspecto adicional foi trazido por Resp7-P, que comentou acerca de aspectos sobre os quais as políticas não têm muito alcance, já que estas são mais focadas nos prontuários, que, no entanto, não são a única fonte de informação sobre os pacientes. Por exemplo, citou as entrevistas feitas na área de Psicologia, que não constituem parte do prontuário, mas contêm informações altamente privadas do paciente.

Sobre a criação e atualização dessas políticas, Resp5-E comentou que confia na forma como essas políticas são redigidas e revisadas e que, no estado, há instituições que são referência pelo processo consciencioso que conduzem. No entanto não tem tanto confiança em relação ao quanto essas políticas são seguidas. Resp1-M comentou que esse processo é feito com bastante cuidado pelas instituições, mas compartilha da ideia de Resp5-E em relação ao atendimento dessas políticas. Isso denota uma ligação com os desafios citados anteriormente de que o componente humano precisa aderir a essas políticas e de que o processo de controle do seguimento dessas políticas precisa ser melhorado. Resp3-M comenta que se sente muito confortável com a forma como as políticas da sua organização são atualizadas, opinião compartilhada por Resp6-B. No entanto esse último reforça que "não necessariamente isso vá redundar numa mudança de cultura".

A questão seguinte, acerca de responsabilidades dos profissionais de saúde, no sentido de preservar a privacidade dos registros dos pacientes, trouxe questões de certa forma contraditórias em relação à resposta à pergunta anterior. Resp3-M comentou que as responsabilidades "são mais subjetivas, não existe acordo tácito, mas se procura respeitar a legislação vigente". A contradição surge tendo em vista que as políticas são (ou ao menos deveriam ser) feitas com base na legislação, então não são questões tácitas e sim explícitas nas políticas. Resp1-M reforça que há na area um "segredo instrumental", de que por vezes o que se compartilha com um colega, como narrando um fato ocorrido, não é ficção, são fatos reais sobre pessoas reais, então o profissional precisa se ater ao compartilhamento do que é fundamental para o atendimento. Resp2-M lembra que as responsabilidades pelo

sigilo devem ser compartilhadas com todos os que fazem uso da informação, desde o pessoal da área administrativa, que insere as informações dos pacientes, até os da área de TI, que têm acesso a elas. Esses funcionários devem igualmente assinar um termo de responsabilidade em relação ao sigilo da informação. Resp4-E alega um importante aspecto, que são os comentários em áreas comuns de hospitais ou clínicas médicas. Mesmo que o nome completo da pessoa não seja citado, outros dados de identificação podem ser citados e, na união dessas informações, é possível deduzir qual pessoa está internada e por qual motivo. Segundo o mesmo respondente, em casos de estudos gerados em hospitais corre-se especial risco de violação da privacidade, já que nessa situação o conjunto de informações compartilhadas é grande e os dados de identificação podem contribuir sobremaneira para a violação da privacidade. Resp7-P comenta a importância de que, em situações onde alunos estiverem atuando conjuntamente com a equipe, é necessária a supervisão no acesso às informações, em virtude de que a falta de experiência pode contribuir para o não entendimento da gravidade da violação do sigilo de informações. Esse aspecto corrobora a declaração anterior de Resp4-E. Isso não significa que profissionais experientes possam dar menos valor aos cuidados com o sigilo da informação, justamente por considerarem que, pela experiência que têm, não cairão em armadilhas relacionadas a violão da segurança.

Acerca da capacitação relativa à privacidade das informações dos pacientes, Resp7-P pondera que normalmente não há, nas instituições, um programa de capacitação específica em relação a esse aspecto e que essa qualificação limita-se à formação profissional. Resp6-B comenta que as instituições mais preocupadas com esse aspecto promovem capacitações para seu pessoal, mas que nem sempre é dada a devida atenção pelas equipes a isso, já que “sempre há um aspecto mais importante – na visão deles – a resolver”. Para Resp2-M, boa parte dessa qualificação fica a cargo dos comitês de ética das instituições. No entanto nem sempre estes movimentam-se no sentido das mudanças culturais necessárias, tratando mais de aspectos normativos do que mudança de visão a respeito do assunto. Resp1-M ressalta a necessidade de formação continuada para cada profissional, no sentido de que “a cada dois ou três anos cada funcionário tenha contato com o tema e passe por essa capacitação”, já que os desafios mudam, os riscos evoluem, e os profissionais também precisam evoluir da mesma forma.

Ainda no mesmo aspecto, abordou-se se ,na formação regular, os profissionais tiveram visões um pouco distintas. Resp7-B diz que desconhece capacitações nesse sentido na organização na qual trabalha. Resp2-M cita que as capacitações existem, sem se delongar sobre a efetividade delas. Resp3-M afirma que a formação dada aos profissionais que passam pelo hospital onde trabalha é suficiente. Já Resp6-B é enfático em dizer que não, até por ser um tema complexo e exigindo aprofundamento para passar desse conhecimento para as ações. O respondente comenta que percebe profissionais agindo de maneira incorreta, não por má vontade ou contravenção, mas por descuido, desconhecimento, pressa ou hábito. Resp1-M considera que a organizações esforçam-se nesse sentido, mas que a percepção “do que fazer, e principalmente do que não fazer” é difícil no dia a dia, em cada contato com o paciente ou com os colegas. Resp4-E comenta ainda que “em sala de aula não se tem condições de esgotar todas as dimensões de um assunto”, fazendo-se necessária a criação de mecanismos paralelos para dar conta do assunto.

Na sequência, os respondentes foram questionados a respeito de como os profissionais de saúde procuram seguir as orientações de comportamento seguro no trato das informações de saúde recebidas dentro e fora da instituição. Resp2-M cita alguns exemplos para ilustrar que, se as pessoas estão determinadas a não seguirem as recomendações, elas “dão um jeito para chegarem ao seu objetivo final”. Entre os exemplos, cita um profissional que, ao ser proibido de tirar cópia de um prontuário, fotografou página por página. Resp7-P coloca o fato de que é necessário que os profissionais de saúde tenham um fórum para expor as angústias e assim evitarem “ficar falando isso a amigos ou familiares, que estão fora desse contexto e poderão não ter o zelo necessário com a informação”. Resp6-B cita que é

importante falar o tempo todo no que não pode ser feito, “porque o ser humano é fraco diante de uma possível vantagem, ele logo esquece as recomendações, se achar que terá algum proveito em acessar as informações”. Resp1-M completa dizendo que “tem gente que acha que não faz mal você contar por aí”, que ninguém vai conseguir identificar de quem se está falando.

A última questão perguntou aos respondentes a respeito de uma possível influência de fatores como stress, cansaço, desmotivação no vazamento de informações. Resp3-M citou que acredita que “uma pessoa sobrecarregada e que tenha responsabilidades poderia com isso abrir mão da privacidade para dar conta de tudo”. Resp4-E considera que estes fatores influenciam, já que, às vezes, não há tempo para agir visando à proteção do paciente. Resp1-M considera que o cansaço ou o stress não são fatores decisivos, mas sim que podem contribuir em um quadro de descuido já existente por parte daquele profissional. Resp2-M concorda, reforçando que atualmente “cansaço e stress já fazem parte do dia-a-dia”. Resp6-B ressalta que os aspectos mais importantes são vinculados ao comportamento humano, já que a relação de atendimento, como colocada no Brasil, é “uma situação de poder, de alguém que tem acesso ao prontuário de alguém e, por veze,s essas pessoas são jovens demais para terem amadurecido isso”. Resp7-P lembra que nem todos os seres humanos sensibilizam-se da mesma forma a respeito das consequências de um possível vazamento de informações de um paciente.

Os resultados mostram que, de maneira geral, a questão não é abordada adequadamente, especialmente porque os aspectos comportamentais não são amplamente considerados na elaboração das políticas. No item a seguir, faz-se uma reflexão da relação dos achados da pesquisa com a gestão da informação.

4.3 Implicações para a área de Administração da Informação

A área de administração da informação nas organizações normalmente observa todos os mecanismos relacionados à manutenção dessa informação como uma informação íntegra e disponível para os usos que dela dependem. Nesse sentido, a segurança da informação precisa observar aspectos técnicos e de gestão como aqueles mais relacionados com aspectos subjetivos, assim como é a questão de privacidade e sigilo das informações. A seguir, procede-se a uma reflexão das implicações para a área, com base na interpretação dos dados oriundos das entrevistas. A quantidade de citações pode ser diferente do número de entrevistas em virtude de comentários a mais (ou menos) de uma categoria.

A primeira implicação dá-se em relação aos desafios relacionados à privacidade de informações de pacientes da área médica, conforme a QUADRO 2, a seguir.

QUADRO 2 – Desafios relacionados à privacidade

Categoria	Principais itens (na visão dos entrevistados)	Citações
Tecnológicos	▪ Impedir o acesso não autorizado às informações de pacientes.	1
Comportamentais	▪ Formação da compreensão do significado de sigilo e privacidade. ▪ Entendimento da motivação do acesso não autorizado. ▪ Capacitações que permitam uma mudança da cultura de acesso onipotente e não punição. ▪ Os comentários dos profissionais em áreas comuns podem ser a maior fonte de quebra de sigilo.	5
	▪ A percepção do que é lícito é difícil no dia a dia em cada contato com o paciente ou com os colegas.	2
Mecanismos de proteção	▪ Definição mais clara de regras de acesso às informações (inclusive para documentos em papel).	3

Fonte: Elaborado pelos autores com os dados da pesquisa

Observa-se que, na visão dos respondentes, não se trata de um problema relacionado à tecnologia, mas sim a aspectos comportamentais dos indivíduos envolvidos. Nesse sentido,

faz-se necessário analisar de maneira mais aprofundada quais são as possíveis formas de modificar esse comportamento e introduzir, paulatinamente, uma mudança cultural. A definição de mecanismos de proteção igualmente só funcionará com uma cultura que valoriza e respeita a privacidade de informações de pacientes.

A segunda implicação se dá em relação aos desafios relacionados à privacidade de informações de pacientes da área médica, conforme a QUADRO 3, a seguir.

QUADRO 3 – Políticas de acesso e uso de informações privadas

Categoria	Principais itens (na visão dos entrevistados)	Citações
Existência	▪ As políticas normalmente existem (mas não necessariamente são efetivas). ▪ Há regras táticas, mas não necessariamente explícitas (registradas em documentos).	5
Observância pelos profissionais	▪ As políticas são adequadamente seguidas. ▪ As políticas são parcialmente observadas, ocorrendo há uma relativização por parte do profissional. ▪ O profissional considera uma possível punição *versus* uma possível recompensa (especialmente porque a punição é branda). ▪ Há a necessidade de aumentar o controle sobre a observância dessas políticas. ▪ Se o profissional estiver disposto a burlar as regras, ele encontrará uma forma.	1 4 2 2
Atualização e completude	▪ As políticas não abordam a totalidade de aspectos relacionados à privacidade das informações. ▪ As políticas são adequadamente atualizadas.	3 4

Fonte: Elaborado pelos autores com os dados da pesquisa

A existência de políticas de acesso e uso de informações privadas é algo bem presente nas organizações. No entanto isso não significa que estas sejam adequadamente seguidas pelas profissionais, até em virtude das questões culturais expostas anteriormente. A relativização das regras por parte dos profissionais é preocupante, já que pode ocorrer o balanço entre punição e recompensa, o que pode comprometer ainda mais o seguimento dessas políticas. Dessa forma, as políticas elaboradas pela área de TI podem se tornar inócuas, deixando a empresa desprotegida para outras relativizações de segurança da informação.

A terceira implicação se dá em relação à responsabilidade e desafios relacionados à privacidade de informações de pacientes da área médica, conforme a QUADRO 4, a seguir.

QUADRO 4 – Responsabilidade dos profissionais envolvidos

Categoria	Principais itens (na visão dos entrevistados)	Citações
Entendimento das próprias responsabilidades	• As responsabilidades são tácitas (e não explícitas nas políticas). • O entendimento é de que os comentários com colegas não envolvidos no caso não constituem quebra de sigilo. • A responsabilidade deve ser compartilhada entre todos os que têm contato com a informação, incluindo a área administrativa e TI. • Supervisão de professores, quando alunos estiverem atuando, em virtude da pouca experiência desses profissionais.	1 2 3 1

Fonte: Elaborado pelos autores com os dados da pesquisa

O aspecto que mais preocupa é o entendimento das próprias responsabilidades por parte daqueles que manuseiam essas informações, entendimento este bastante flexibilizado em termos de o que pode e o que não pode ser feito em termos de acesso e uso das informações privadas. Para a área de TI, a preocupação é se as capacitações abordam

adequadamente as responsabilidades dessa área, permitindo que os profissionais de TI tenham uma noção mais clara de suas responsabilidades.

A quarta implicação dá-se em relação à capacitação, no sentido de que os profissionais estejam preparados para os desafios relacionados à privacidade de informações de pacientes da área médica, conforme a QUADRO 5, a seguir.

QUADRO 5 – Capacitação dos profissionais envolvidos em vista às responsabilidades

Categoria	Principais itens (na visão dos entrevistados)	Citações
Abordagens	• Ocorrem treinamentos isolados, mas não exatamente um programa de formação.	2
	• Necessidade de formação continuada para cada profissional, pois os riscos e desafios mudam.	2
	• A capacitação deve ser aprofundada a ponto de iniciar uma mudança cultural.	1
	• As capacitações existem, mas não há uma preocupação significativa com a sua efetividade.	3
Participação dos profissionais	• Os participantes de uma capacitação têm dificuldade de se dedicarem a ela, sempre havendo outro assunto urgente a tratar.	2
Formação	• Na formação regular, é difícil esgotar o assunto, fazendo-se necessária a criação de mecanismos paralelos para dar conta do assunto.	2

Fonte: Elaborado pelos autores com os dados da pesquisa

Em relação à capacitação, há a necessidade de desenvolver programas de capacitação adequados para cada grupo de profissionais, no sentido de que cada um entenda claramente qual o seu papel e suas responsabilidades no processo. Para a área de TI, fica complicado um objetivo de estar *compliance* com um regulatório, se vários outros atores do processo não estiverem envolvidos e aderentes a práticas de Segurança da Informação.

5 - Considerações Finais

Os resultados deste trabalho têm como intuito complementar o conhecimento sobre aspectos técnicos e de gestão da Segurança da Informação (normalmente abordados via Política de Segurança da Informação) já existente na área O resultado da pesquisa pode contribuir na melhor compreensão de aspectos adjacentes à segurança da informação, permitindo a elaboração de políticas de segurança mais efetivas. Nesse sentido, os resultados mostraram deficiências significativas acerca do encaminhamento dado para o problema de segurança e privacidade em informações de saúde.

Como pesquisas futuras, pretende-se conduzir uma pesquisa *survey* com profissionais da área médica. Para tanto, é importante entender a compreensão desses profissionais acerca de aspectos relacionados à Segurança da Informação, como a privacidade das informações. Sem a investigação com profundidade sobre os elementos que compõem o tema central da pesquisa, o instrumento proposto para a *survey* possivelmente ficaria apenas com a visão dos profissionais que trabalham com informação, sem considerar todos os aspectos subjacentes à área médica. Como limites para esta pesquisa, podem-se citar a reduzida quantidade de entrevistados e o fato destes pertencerem a um número reduzido de organizações.

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 16 de agosto de 2009.

ACQUISTI, A.; GROSSKLAGS, J. *Losses, gains and hyperbolic discounting*: An experimental approach to information security attitudes and behavior, in Camp, J. Lewis, S. eds. The economics of information security, 2004. Originally presented at the 2003 workshop on economics and information security (WEIS '03).

ACQUISTI, A.; GROSSKLAGS, J. *What can behavioral economics teach us about privacy?*, Digital Privacy: Theory, Technologies and Practices. Taylor and Francis Group, 2007.

ALBRECHTSEN, E. A qualitative study of users´ view in Information Security. *Computers & Security,* v. 26, n. 4, p. 276-289, Jun., 2007.

BARDIN, L. *Análise de conteúdo*. Lisboa: Edições 70, 1977.

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

CHO, V. A study of the roles of trusts and risks in information-oriented online legal services using an integrated model, *Information & Management*, v.43, n.4, p. 502-520, 2006.

D'ARCY, J., HOVAV, A., GALLETTA, D. User awareness of security countermeasures and its impact on Information Systems misuse: a deterrence approach, *Information Systems Research,* v.20, n.1, p. 79-98. 2009.

DHILLON, G; BACKHOUSE, J. Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal*, v. 11, n. 2, p. 127-154, 2001.

DYSON, E. *A Sociedade Digital.* Um roteiro da vida na internet. Rio de Janeiro: Campus, 1998.

FONTES, E. *Segurança da Informação*: o usuário faz a diferença, Rio de Janeiro: Editora Saraiva, 2006.

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

GOLDIN, J. R.; FRANCISCONI, X. *Bioética*. Disponível em http://www.ufrgs.br/bioetica/provac.ppt#9. Acesso em 01 de julho de 2009.

JANCZEWSKI, L.; SHI, F. X. Development of Information Security Baselines for Healthcare Information Systems in New Zealand, *Computer & Security*, v. 21, n. 2, p. 172-192, 2002.

MANDARINI, M. *Segurança Corporativa Estratégica*. São Paulo: Manole, 2004.

MOREIRA, N. S. *Segurança Mínima*: Uma visão corporativa da Segurança da Informação, Rio de Janeiro: Axcel Books, 2001.

NG, B. Y.; KANKANHALLI, A.; XU, Y. *Studying users' computer security behavior*: a health belief perspective, Decision Support Systems, v. 46, n. 4, p. 815-825, 2009.

OLIVEIRA, L.; JANSSEN, L. A. *Proposta para Avaliação de Maturidade de Processos de Gestão de Segurança da Informação em Instituições Hospitalares*, I Encontro de Administração da Informação, 24-26, out., Florianópolis, 2007.

RANSBOTHAM, S., MITRA, S. Choice and Chance: a conceptual model of paths to information security compromise, *Information Systems Research*, v.20, n.1, p.121-139, 2009.

ROSE, E. A. An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, v. 43, 3, p. 322-335, 2006.

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

SILVA, J, A. *Curso de Direito Constitucional Positivo*, 19ª Ed. p. 206. São Paulo: Malheiros, 2001.

SWANSON, J. A. *The public and the private in Aristotle´s political philosophy*. Cornell University Press, 1992.

WESTIN, A. F. *Privacy and Freedom*. New York: Atheneum, 1967.

WILLIAMS, P. A. Information Security Governance, *Information Security Technical Report*. v. 6, n. 3 p. 60-70, 2001.