

PRONTUÁRIOS ELETRÔNICOS E PRIVACIDADE DE INFORMAÇÃO NA CIÊNCIA MÉDICA

DALL'ASTA, Heloísa Bonatto.¹

DO MAR, Sara Mendes.²

MAGNAGNAGNO, Odirlei Antonio.³

RESUMO

No presente artigo discute-se como os avanços tecnológicos podem facilitar e auxiliar o princípio da privacidade na relação médico-paciente, como essa relação pode se manter no uso de prontuários eletrônicos do paciente, quais os critérios utilizados no rompimento do sigilo médico envolvendo a ética médica e a segurança, além disso trata também da equivalência entre privacidade e confidencialidade nas relações entre os profissionais de saúde e os usuário e também de como essa quebra de confidencialidade afeta a confiança do paciente. Junto a isso se comenta a maneira como, muitas vezes, as informações reveladas mediante a confidencialidade que se estabelece numa relação clínica, são usadas de forma inapropriada causando constrangimento e danos aos usuários dos sistemas de saúde e, consequentemente, aos profissionais que se dedicam a esses pacientes. A metodologia baseia-se em várias fontes bibliográficas e possui caráter teórico-reflexivo. Assim conclui-se que o uso destas tecnologias, no âmbito da saúde, auxiliam o trabalho destes profissionais, no entanto elas ainda requerem um melhor sistema de segurança para a manutenção do sigilo médico-paciente.

PALAVRAS-CHAVE: privacidade, segurança, prontuário eletrônico, ética médica.

RECORDS ELECTRONIC INFORMATION AND PRIVACY IN MEDICAL SCIENCE

ABSTRACT

In this article we discuss how technological advances can facilitate and help the principle of privacy in the doctor-patient relationship, how this relationship can be maintained in the use of electronic medical records of the patient, the criteria used in breach of medical confidentiality involving medical ethics and safety furthermore also deals with the equivalence between privacy and confidentiality in the relations between health professionals and users and also how this affects confidence break the confidence of the patient. Along with it is said how, often, the information revealed by the confidentiality that is established in a clinical relationship are used inappropriately causing embarrassment and damage to the users of health systems and, consequently, to the professionals who are dedicated to these patients. The methodology is based on various literature sources and has theoretical and reflective character. Thus we conclude that the use of these technologies in health, assist the work of these professionals, however they still require a better security system for the maintenance of doctor-patient confidentiality.

PALAVRAS CHAVE EM LÍNGUA ESTRANGEIRA: privacy, safety, electronic medical records, medical ethics.

1. INTRODUÇÃO

As ciências em saúde discutem os princípios éticos na relação entre profissionais e usuários há algum tempo. Um dos pioneiros deste estudo foi Hipócrates, o qual criou o juramento hipocrático, que visava defender o direito dos doentes em relação a suas informações passadas aos profissionais de saúde, ou seja, a privacidade e a confidencialidade (SOARES e DALL'AGNOL, 2011). A privacidade é um direito individual que protege o indivíduo, já que limita o acesso às suas informações. E a confidencialidade é a garantia de que esse conhecimento não será transmitido sem aceitação prévia do paciente.

Com a era da tecnologia, mesmo diante de tantas desigualdades sociais, políticas e econômicas, há um favorecimento do armazenamento, da distribuição e do rápido acesso às informações, acarretando um crescimento significativo da aplicação desses recursos nas áreas da saúde por meio de prontuário eletrônico do paciente, internet em saúde, sistemas de apoio à decisão e telemedicina. Dentre esses, o prontuário eletrônico é o meio que mais facilita a vida dos profissionais da saúde, já que ele permite o rápido acesso às informações preegressas e importantes do paciente, além de que pode se ter acesso a tratamentos e conclusões obtidas por diferentes médicos e agentes da saúde (MAGNAGNAGNO, 2015).

A partir disso permitiu-se que muitos profissionais, não só da saúde, pudessem ter acesso às mais variadas informações dos usuários do sistema de saúde: características físicas e psicológicas, hábitos de vida, enfermidades preegressas entre outras informações sigilosas. Com o valor estratégico conferido à informação e a conexão da sociedade em rede, surgem, além de inúmeras facilidades e benefícios, algumas questões éticas a serem discutidas e avaliadas (GAERTNER e SILVA, 2005). Uma delas é a privacidade da informação, um grande desafio e assunto de interesse de toda a sociedade. Com isso surge uma necessidade de se estabelecer limites sobre quem pode ter acesso a essas informações, como elas são utilizadas e mediante quais critérios elas podem ser divulgadas - com ou sem autorização do paciente -, visto que o mau uso desses conhecimentos acarreta constrangimento ao paciente, perda da confiança na relação médico-paciente e pode até levar a disputas judiciais.

¹Acadêmica do curso de medicina da Fundação Assis Gurgacz. E-mail: heho_bd@hotmail.com

²Acadêmica do curso de medicina da Fundação Assis Gurgacz. E-mail: mendesara11@hotmail.com

³Orientador e professor da matéria de Tecnologia de Informação e Comunicação da Fundação Assis Gurgacz. E-mail: odirlei@fag.edu.br

Assim esse artigo tem como foco principal o estabelecimento de práticas no âmbito da saúde que potencializem a autonomia dos cidadãos e os protejam de possíveis abusos que firam sua dignidade (FORTES, 2000). Além disso elucidar sobre a ética da equipe de saúde evitando o mau uso das informações e estabelecer mecanismos que limitem o acesso a esse conhecimento e, consequentemente, fornecer ao usuário dos serviços de saúde maior segurança e privacidade, conservando suas informações de maneira a não ferir seus direitos.

2. FUNDAMENTAÇÃO TEÓRICA

Há muito tempo vem se discutindo os princípios bioéticos, os quais são beneficência, não maleficência, autonomia e justiça. Entre estes, destaca-se a autonomia, que é a capacidade do indivíduo decidir o que é melhor para ele, tal princípio não se relaciona para crianças e para pessoas que não possuem essa capacidade de julgar claramente, por exemplo, pessoas que possuem uma doença psiquiátrica e também a autonomia de tirar a própria vida. Segundo Fortes,

A todo cidadão deve ser permitida a expressão e o exercício da autodeterminação, que se desenvolva em função de suas convicções pessoais, sempre que estas não interfiram na liberdade dos demais, pois é da perspectiva do sujeito que as ações são consideradas autônomas ou não (FORTES, 2000, p. 308).

A palavra privacidade deriva etimologicamente do adjetivo "privatividade", ou seja, o "caráter do que é privativo, próprio de alguém, só dele, não público, reservado, de foro íntimo" (FORTES, 2000, p. 309). Simionato, Sant'ana e Santos (2013, p. 4) complementam ainda que "na legislação brasileira a privacidade está ligada com intimidade, o direito à intimidade tem sido denominado como direito ao resguardo, ao recato, ao segredo, à vida ou esfera privada ou íntima". Porém, Fortes (2000) reitera e afirma que esta definição não é aceita universalmente já que vários conjuntos a envolve, como por exemplo, exclusão, anonimato, solidão, segredo e outros mais. Diante disso o conceito de privacidade mostra dois enfoques: o primeiro centra-se no controle que o indivíduo exerce sobre o acesso de outros a si próprio e o segundo, define a privacidade como uma condição ou estado de intimidade (LOCH, 2006).

"O ser humano deve ter o direito à privacidade igualmente ao direito à intimidade, tendo garantido o controle sobre quem e como ocorre o acesso às informações que consideram pessoais, preservando informações particulares que o indivíduo tenha interesse de manter em sigilo" (SIMIONATO, SANT'ANA e SANTOS, 2013, p. 5). A privacidade é fundamental na proteção do ser humano, não somente como escudo contra o exterior, mas como elemento positivo, indutor da cidadania e dos direitos de liberdade de uma forma geral (SIMIONATO, SANT'ANA e SANTOS, 2013 *apud* DONEDA, 2006, p.146). Em conjunto a isso ela auxilia no estabelecimento de um vínculo entre o médico e o paciente.

Loch (2006) afirma que há o estabelecimento duas formas de confidencialidade nas relações clínicas, a primeira é baseada na relação interpessoal, onde a manutenção do segredo é passível de ser completa, bastando o comprometimento das pessoas que compartilham a informação, já a segunda é a confidencialidade do registro desta informação.

Hipócrates foi o primeiro a estudar a privacidade como um exercício da profissão médica e afirma "e o que quer que eu veja ou ouça no curso de minha profissão, assim como fora de minha profissão, nos meus encontros com homens, se for algo que não deve ser publicado fora, eu jamais divulgarei, considerando essas coisas como segredos sagrados" (FORTES, 2000, p. 309). "A ética de Hipócrates destaca-se no Juramento Hipocrático, considerado como fundamento para origem da ética dos profissionais de saúde" (SOARES e DALL'AGNOL, 2011, p. 684). Loch (2006) também ressalta a importância do sigilo médico, que tem raízes no século V a.C. baseado nesse juramento, onde mostra que essa prática deve ser cumprida pelo médico para proteger o segredo dos doentes.

A partir da concepção hipocrática, o segredo médico tem se mantido na tradição da profissão médica, mesmo que modificado e restrito em sua aplicação. É no século XIX que surgem os primeiros Códigos Deontológicos na medicina - são condutas dos deveres e da moral médica - regulamentando a profissão e reafirmando o segredo como obrigação de ofício. No século XX o movimento dos Direitos Humanos, através da Declaração Universal dos Direitos Humanos, promulgada em 1948, pela ONU, cita explicitamente o direito à não interferência na vida privada pessoal ou familiar (LOCH, 2006). Mas isso só é aplicado concretamente à medicina no final dos anos 60 e início dos anos 70, com o primeiro documento formulado com o intuito de defender o princípio da privacidade, o "Patient's Bill of Rights" (Declaração dos Direitos dos Pacientes), emitido pela Associação Americana de Hospitais que expressava: o paciente tem o direito de esperar que todas as suas comunicações e dados sejam tratados como confidenciais" (FORTES, 2000, p. 312).

Após este documento vários países também passaram a defender tal conceito. Em Lisboa, surge uma Declaração sobre os Direitos do Paciente pela Associação Médica Mundial, na década de 80, a qual segundo Fortes (2000),

Se manifestou pelo direito do paciente a esperar que se respeite a natureza confidencial de todos os dados médicos pessoais que lhe concernem. Também a Carta Européia dos Direitos dos Pacientes, do Parlamento Europeu, de 1984, contemplou o segredo profissional como um dos direitos a ser preservado e que somente poderia ser attenuado por motivos graves perfeitamente definidos em seus limites (FORTES, 2000, p. 313).

No Brasil através da Constituição Federal de 1988 este foi implantado, afirmando que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação” (FORTES, 2000, p. 313). Além da Constituição foi complementado o Código Penal, o qual tem por dever punir o vazamento dessas informações ilícitas nos seguintes casos,

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

§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos Sistemas de Informação ou banco de dados da Administração Pública (MIRABETE e FABRINNI, 2013, p. 1016).

Art. 154 - Divulgação de informações obtidas no exercício de atividade profissional, incluindo entre os tipos penais a revelação, sem justa causa, de segredo do qual se teve conhecimento em razão de função, ministério, ofício ou profissão, e cuja revelação possa causar dano a alguém (MIRABETE e FABRINNI, 2013, p. 1019).

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (MIRABETE e FABRINNI, 2013, p. 1023).

Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação (MIRABETE e FABRINNI, 2013, p. 2022).

Assim em nossa contemporaneidade “a garantia da preservação do segredo das informações, além de uma obrigação legal contida no Código Penal e na maioria dos Códigos de Ética Profissional, é um dever *prima facie* de todos os profissionais e também das instituições” (GOLDIM e FRANCISCONI, 1998, p. 1). Goldin cita Sir David Ross, o qual afirmava “O dever *prima facie* é uma obrigação que se deve cumprir, a menos que conflite, numa situação particular, com um outro dever de igual ou maior porte” (GOLDIM e FRANCISCONI, 1998, p. 1), ou seja, o médico terá o dever de analisar o fator risco-benefício. Segundo o Conselho Regional de Medicina a quebra do sigilo ocorrerá quando,

A revelação do segredo médico é permitida nos casos de abuso e/ou sevícia sexual para apurar responsabilidades; nas doenças de notificação compulsória; nos defeitos físicos ou doenças que ensejam erro essencial quanto a pessoa e levem à nulidade de casamento; nos crimes que não impliquem em processo do paciente; na cobrança judicial de honorários; ao testemunhar o médico para evitar injustiça; nas perícias médicas; nos exames biométricos admissionais e previdenciárias e nos exames de sanidade mental para seguradoras (CRM, 2000, p. 2).

Assim presentemente a comunidade científica tenta minimizar os prejuízos advindos do progresso científico, questões como genética humana, AIDS, levam a reflexão sobre privacidade e confidencialidade médica.

Quanto à prática científica há também normas que garantem o sigilo das informações genéticas sobre as técnicas utilizadas e a possibilidade de doenças futuras, isso porque tal conhecimento não gera danos somente ao paciente, mas aos seus descendentes também, e a omissão destas informações evitam práticas discriminatórias, com isso segundo (FORTES, 2000),

Nos Estados Unidos, foi proposto o "Genetic Privacy Act", como legislação federal, por considerar-se que a informação genética é de natureza diferente de outros tipos de informação pessoal. Deste modo, requer proteção especial, pois a análise genética do DNA possibilita que se conheça o futuro provável de uma pessoa, particularmente em termos físicos e bem-estar mental (FORTES, 2000, p. 313).

Na União Europeia, mediante a "Convenção para a Proteção dos Direitos do Homem e da Dignidade Humana frente às Aplicações da Biologia e da Medicina", afirma Fortes (2000), eles se atentam para proteger dignamente a identidade do ser humano. Já no Brasil, não existe nenhuma convenção composta especificamente para isto, assim há uma preocupação em relação à privacidade por parte das pessoas estudadas.

Concomitantemente estudos Antropológicos também afirmam que mesmo em diferentes culturas o aspecto da privacidade ainda é mantido. E profissionais da Psicologia afirmam que “o ser humano necessita possuir áreas secretas para manter seu equilíbrio psíquico” (FORTES, 2000, p.309). Por isso, tanto legal quanto éticamente, privacidade se refere ao limite de acesso de terceiros ao corpo ou mente de alguém, seja através de contato físico ou da revelação de pensamentos ou sentimentos (GOSTIN et. al, 1993).

A confidencialidade e a privacidade estão diretamente relacionadas, pois privacidade é sinônimo de segredo, é uma responsabilidade do médico, onde o paciente determina o que pode e o que não pode ser compartilhado. Já a confidencialidade é a garantia de que estas informações não serão reveladas sem a autorização prévia da pessoa, ou seja, é o “princípio da confidencialidade das informações que gera no profissional o dever ético e legal de resguardá-las” (FORTES, 2000, p. 310).

Os fatores para se preservar a intimidade surgem, segundo Fortes (2000), com o advento da burguesia como classe social e com o avanço tecnológico que aumentou as possibilidades de violação do território da intimidade da pessoa humana. Assim, foi constituída uma maneira do indivíduo ser “deixado em paz” e uma forma da pessoa ser

amparada da pressão social, baseado em Kant que afirma que para isto é preciso três exigências: “a solidão (o desejo de estar só); o segredo (a exigência de sigilo) e a autonomia (a liberdade de decidir sobre si mesmo, como centro do qual derivam as informações) ” (FORTES, 2000, p. 312).

No Brasil, legalmente, o sigilo e a privacidade de informação estão garantidos pelo Código Penal Brasileiro que, em seu artigo 154, trata do crime de violação do segredo profissional o qual se estende a qualquer profissão. O Código de Ética Médica regulamenta várias situações específicas onde é vedado ao médico a revelação de informações, ficando contemplada a quebra do sigilo somente por justa causa, dever legal ou autorização expressa do paciente (LOCH, 2006).

Com o avanço tecnológico, houve um crescimento significativo das aplicações de informática na área da saúde, alguns exemplos são: Prontuário Eletrônico do Paciente (PEP), Internet em Saúde, Sistemas de Apoio à Decisão e Telemedicina (SALVADOR e ALMEIDA FILHO, 2005). Com essas novas tecnologias surgem novos meios de comunicação e de informação que favorecem o armazenamento, a transmissão e a distribuição de dados. O fluxo de informações permite que grandes volumes de dados possam ser obtidos e armazenados, abrangendo tanto indivíduos quanto organizações. Se adequadamente tratados e usados, esses dados criarião um novo universo de possibilidades de fonte de informações, já que cada informação possui um grande valor agregado e pode traçar o perfil de cada indivíduo, ilustrando suas características físicas e até hábitos de vida (SIMIONATO, SANT'ANA e SANTOS, 2013).

Tudo o que é divulgado na rede está armazenado formando uma “sombra de dados”, que pode viabilizar a construção de uma imagem digital de cada um de nós. Devido a isso é necessário que os usuários estejam atentos a suas atividades e garantam os seus direitos de consumidores, usuários e cidadãos, buscando a privacidade de sua sombra de dados, no intuito de manter a segurança e a preservação de sua imagem digital (SIMIONATO, SANT'ANA e SANTOS, 2013). Contudo, com o avanço tecnológico, a estruturação do direito à privacidade se apresenta cada vez mais frágil.

A forma de armazenamento mais promissora nas instituições de saúde é o PEP⁴, que é uma ferramenta fundamental para profissionais de saúde e para gestores hospitalares, já que por meio desse recurso podem-se controlar, de maneira eficiente, todas as informações pessoais e administrativas relacionadas ao paciente. Além disso, podem conhecer os custos, lucros e prejuízos ocorridos dentro de determinado período de tempo, recursos materiais e humanos alocados, assim como utilizá-lo para fazer previsões de investimentos a médio e longo prazo. O PEP foi criado com o objetivo de facilitar o trabalho de médicos e enfermeiros. A partir dele esses profissionais podem recordar de forma sistemática os fatos e eventos clínicos ocorridos em um indivíduo e também fazer com que os demais profissionais da saúde envolvidos no processo de atenção possam ter acesso a estas informações (SALVADOR e ALMEIDA FILHO, 2005).

Ainda segundo Salvador e Almeida Filho (2005), prontuário eletrônico do paciente define-se por ser um registro clínico e administrativo informatizado da saúde e doença do paciente desde seu nascimento até sua morte. Dentro de um sistema utilizado para apoiar os usuários, disponibilizando acesso a um completo conjunto de dados corretos, alertas e sistemas de apoio à decisão. Ele deve conter dados pessoais, histórico familiar, doenças anteriores, hábitos de vida, alergias, imunizações, medicamentos que faz uso, medicamentos e tratamentos anteriores.

O PEP possui vantagens e desvantagens, entre os pontos positivos então: o rápido acesso aos problemas de saúde e intervenções atuais, eliminação da redundância de dados e pedidos de exames, fim da redigitação de informações, integração com outros sistemas de informação, melhor organização, melhoria da efetividade do cuidado contribuindo para uma obtenção de melhores resultados dos tratamentos realizados, ajuda a evitar uma desatenção a detalhes importantes e permite uma busca coletiva. Por outro lado, os pontos negativos se constituem de: necessidade de grandes investimentos de *hardware*, *software* e treinamento; resistência dos profissionais da saúde ao uso de sistemas informatizados; demora para se obter reais resultados da implantação do PEP; sujeito a falhas de *hardware*, redes e *software*, deixando o sistema inoperante; seu uso e acesso indevidos podem colocar a questão da confiabilidade e segurança das informações do paciente em risco (COSTA, 2003).

Contradicoriatamente, segundo Salvador e Almeida Filho (2005), as facilidades dos recursos informáticos muitas vezes são utilizadas de maneira controversa facilitando o extravio e o acesso indevido das informações sobre o paciente. Além disso, os sistemas que utilizam redes de computadores tornam estes dados vulneráveis à acessos não autorizados e a facilidade de alteração de dados registrados eletronicamente traz perigos adicionais à vida e ao bem estar dos pacientes, além de facilitar a fraude. “Um grande problema destes sistemas informatizados de consultórios e hospitais, em questões clínicas e administrativas, é que eles, em sua grande maioria, não priorizam a confidencialidade e a segurança de informações dos pacientes” (SALVADOR e ALMEIDA FILHO, 2005, p. 2).

A confidencialidade das informações do PEP é um direito de todo cidadão, com respaldo na Constituição Federal de 1988, em seu artigo 5º, inciso X que garante a inviolabilidade da intimidade, da vida privada, da imagem e da honra das pessoas. Este dever de preservação de segredo é previsto no nosso Código Penal, artigo 154, e na maioria dos códigos de ética profissional da saúde (SALVADOR e ALMEIDA FILHO, 2005, p. 3).

⁴ Prontuário Eletrônico do Paciente

Isto posto devem ser considerados o uso indevido ou mau uso da informação pelas instituições responsáveis, ocorrendo o acesso inapropriado por usuário do próprio hospital ou acesso de usuários não autorizados. Devido a isso há necessidade de se criar políticas e práticas bem estruturadas de acesso a estas informações, objetivando a conscientização das pessoas de direito a um uso apropriado e seguro de sistemas informatizados (SALVADOR e ALMEIDA FILHO, 2005). Loch (2006) completa que:

O conflito de obter, utilizar e eventualmente compartilhar a informação para proporcionar os melhores cuidados em saúde, sem violar a privacidade do paciente, é uma questão muito complexa em si mesma, demandando a análise de várias classes de valores e princípios morais, de direitos e deveres, de todas as circunstâncias e de todas as consequências que permeiam a relação clínica (LOCH, 2006, p. 60).

As leis e códigos nacionais que se referem aos aspectos legais do PEP são: Declaração Universal dos Direitos do Homem, Código de Ética Médica, Resoluções do CFM, Constituição Brasileira, Novo Código Civil Brasileiro, Código Penal Brasileiro, Política Nacional de Segurança de Informação (SALVADOR e ALMEIDA FILHO, 2005).

Diante disso o profissional da saúde precisa ter um poder de comunicação para que fique claro ao paciente que ele pode falar tudo sobre sua doença que o médico estará lá em sua defesa, criando assim o vínculo entre médico-paciente. Não obstante “o dever de segredo não se limita ao médico, mas a todos aqueles que, em função de sua profissão, tenham acesso a estes dados” (SALVADOR e ALMEIDA FILHO, 2005, p. 4). Em seu estudo Fortes (2000) cita Engelhardt, que afirma que o segredo médico equivale à relação entre cliente e advogado, a qual baseia-se na confiança e na defesa absoluta do segredo, possibilitando um relacionamento mais adequado,

O compromisso hipocrático de confidencialidade oferece uma oportunidade do cliente falar à vontade sobre suas preocupações médicas, que também podem estar vinculadas com o pecado e a violação das leis. Isso pode não só levar a um tratamento mais adequado dos pacientes, mas também dará destaque ao valor especial de reconhecer os enclaves de segurança e privacidade contra as possíveis intromissões do Estado (FORTES, 2000, p. 311).

Dessa forma, a privacidade não se limita apenas na informação, mas sim em um relacionamento. O paciente com condições de analisar e julgar o que é o melhor para si, pode decidir quais informações quer que o médico omita e quais deseja que este comunique. Só o consentimento do paciente poderia autorizar a revelação do conteúdo do prontuário, através do princípio da Autonomia, no qual, o paciente tem o direito de ser responsável por seus atos, de exercer seu direito de escolha respeitando-se sua vontade, valores e crenças, reconhecendo seu domínio pela própria vida e o respeito à sua intimidade. Assim o paciente decidiria quais informações quer guardar para si e quais deseja revelar, porém, no próprio Código de Ética Médica, artigo 102, há uma ressalva sobre tal revelação, podendo ser feita “por justa causa, dever legal ou autorização expressa do paciente” (SALVADOR e ALMEIDA FILHO, 2005).

A obrigação de sigilo por parte do profissional e o direito do paciente em manter privadas as informações reveladas, conferem uma dupla natureza à confidencialidade, transformando-a em um direito-dever. A partir disso devem ser analisados os princípios e circunstâncias que justificam a revelação não autorizada das informações, já que a confidencialidade não é uma obrigação absoluta do médico (LOCH, 2006).

Cabe ao indivíduo determinar quando, como e em que extensão a informação dada por ele pode ser transmitida ou revelada. Na área da saúde, a preservação da privacidade permite que o paciente revele a seu médico situações potencialmente embaralhadoras, num ambiente de confiança e com o propósito de cuidados com sua integridade física e emocional. A confidencialidade é, portanto, uma forma de privacidade informacional, que acontece na relação entre o médico e seu paciente. As informações pessoais obtidas no curso deste relacionamento não podem ser comunicadas para terceiros a menos que autorizadas previamente por aquele que revelou. Assim, todas as informações obtidas nesta situação são confidenciais a menos que o paciente permita ou requisite sua revelação à terceiros (LOCH, 2006).

Contudo, as virtudes éticas não são dons naturais, nós nos predisponemos a isso e assim a ética passa a fazer parte do nosso cotidiano, por isso é preciso que os profissionais de saúde se esforcem para que tal princípio vigore, refletindo sobre como irão agir no dia-a-dia do ambiente hospitalar. A ética baseia-se na reflexão das ações dos seres humanos,

Enquanto a moral e a lei estabelecem regras para as ações, a ética busca justificá-las. A ética interpreta, discute, problematiza e investiga valores e princípios na tentativa de responder aos motivos pelos quais devemos agir de determinada maneira (SOARES e DALL'AGNOL, 2011, p. 685).

Em nossa contemporaneidade o que mais se encontra são pacientes que necessitam de um cuidado vindo de uma equipe de saúde e não apenas de um profissional dessa área. Ainda assim é preciso saber restringir as informações, ou seja, a troca destas deve ser limitada de modo que o profissional saiba apenas o que precisa para tratar o paciente. E ainda, segundo Loch (2006), garantir a confidencialidade é da competência dos profissionais de saúde e das instituições, em respeito ao direito individual de privacidade que está diretamente relacionado ao paciente.

Com tais preocupações surgiu as Agentes Comunitárias, as quais devem residir no mesmo bairro em que trabalham, assim vivem o cotidiano da comunidade com uma maior intensidade do que as demais pessoas da Equipe Médica.

Entretanto, em relação à equipe de enfermagem foi realizado um estudo onde foi revelada uma postura inadequada à medida que “seus integrantes realizaram comentários sobre questões relacionadas à sua própria vida pessoal e a respeito dos aspectos do atendimento que realizam a outros pacientes internados” (SOARES e DALL’AGNOL, 2011, p. 686). Tudo isso foi ouvido por pacientes que estavam internados e pelos seus acompanhantes, que revelaram sentir-se muitas vezes que foram tratados com indiferença e que tiveram sua individualidade desconsiderada por essa equipe.

Por isso, é preciso salientar que essa equipe multiprofissional deve promover o respeito e a autonomia dos pacientes. O cuidado com o paciente “implica não apenas proteger a saúde e o bem-estar dos sujeitos envolvidos, mas refletindo-se no respeito à sua dignidade, à privacidade e à autonomia” (SOARES e DALL’AGNOL, 2011, p.688).

Corriqueiramente dezenas de pessoas têm acesso aos prontuários dos pacientes, partilhando uma informação que, originalmente, foi revelada a outro profissional. Esta perda de confidencialidade tem sido considerada benéfica do ponto de vista assistencial, pois visa proporcionar ao doente todos os cuidados disponíveis na instituição para o correto diagnóstico e tratamento de sua enfermidade. Além disso, a obrigação do sigilo se estende a todas essas pessoas que estão envolvidas no tratamento do enfermo (LOCH, 2006).

Através dos meios eletrônicos ficou muito mais simples guardar informações dos pacientes, contudo também ficou mais fácil acessá-las, um estudo realizado na Inglaterra “verificou que 72% do pessoal de enfermagem que respondeu ao inquérito realizado havia utilizado indevidamente o sistema de informática para conhecer informações sobre pacientes que não estavam sob sua responsabilidade profissional” (FORTES, 2000, p. 316). Esse estudo também revelou que o maior motivo do acesso foi apenas curiosidade e não por interesse profissional.

Os dados gerados pela anamnese e o exame físico são como se fossem uma extensão do corpo ou da mente de alguém, já que essas informações podem ser consideradas como as mais íntimas, pessoais e sensíveis sobre uma pessoa. Para que este ato médico não seja considerado um acesso não autorizado, deve ser o paciente, e não o profissional de saúde, quem determina quais destas informações podem ser reveladas. Por isso Garantir a confidencialidade é da competência dos profissionais de saúde e das instituições, em respeito ao direito individual de privacidade que está diretamente relacionado ao paciente (LOCH, 2006).

Hoje os hospitais vêm utilizando prontuários eletrônicos, os quais possuem as informações detalhadas dos pacientes. Isso revela que o conteúdo do prontuário pertence ao paciente, sendo as instituições e os profissionais da saúde responsáveis por sua custódia, o que faz com que eles sejam obrigados a não revelar as informações fornecidas em confidencialidade sem autorização prévia do paciente. Exceto quando estas possam ser utilizadas em função da necessidade de cuidado ao paciente, por justa causa ou dever legal. Além disso, fica sob-responsabilidade das instituições de saúde a implementação e o aprimoramento continuado, estabelecendo normas e rotinas de controle de acesso e identificação de usuários, como parte de um sistema seguro de proteção ao conteúdo do PEP (MOTTA, 2003).

Para se protegerem, muitos utilizam Políticas de Segurança da Informação que é um conjunto de regras com a finalidade de regulamentar e proteger os recursos de um sistema, segundo Magnagnagno (2015) e “sua utilidade é definir as responsabilidades do uso de recursos computacionais”.

Outro fator que auxilia a manter o sigilo e que também é utilizado por estes hospitais, segundo Magnagnagno (2015), são as normas internas feitas pelos hospitais, por exemplo, explicar a gravidade da liberação dessas informações e as normas externas, como a ética médica por exemplo, segundo o Código de Ética Médica em seu 11º artigo,

O médico deve manter sigilo quanto às informações confidenciais de que tiver conhecimento no desempenho de suas funções. O mesmo se aplica ao trabalho em empresas, exceto nos casos em que seu silêncio prejudique ou ponha em risco a saúde do trabalhador ou da comunidade (CRM, 1988, p. 5).

Segundo Magnagnagno (2015), um dos documentos que mais contém meios de proteção é a HIPAA (*health insurance portability and accountability act*) a qual protege os dados do paciente e também protege do uso abusivo das informações do paciente sobre profissionais da saúde,

A lei HIPAA exige que as informações sejam acessadas com usuário e senha individuais aos sistemas, a fim de auditar as alterações realizadas pelo usuário no Prontuário Médico do paciente. A exigência também ocorre nas ferramentas da Tecnologia da Informação, exigindo que os computadores tenham senha de acesso, limitando somente aos usuários liberados, tratando também especificamente de recomendações em relação à privacidade de certas informações de saúde (MAGNAGNAGNO, 2015, p. 36).

A HIPAA é utilizada principalmente nos Estados Unidos, no Brasil foi criada a ANS com o intuito de regulamentar o uso dos dados, a qual segundo afirma,

A finalidade institucional é promover a defesa do interesse público na assistência suplementar à saúde, regular as operadoras setoriais - inclusive quanto às suas relações com prestadores e consumidores - e contribuir para o desenvolvimento das ações de saúde no País, e, além disso, uma de suas competências é a de proceder à integração de informações com os bancos de dados do Sistema Único de Saúde (ANS, 2012, p 2).

A segurança da informação está suportada pelos princípios básicos de: (MARTINS, 2004)

- Integridade: processo de assegurar que recursos ou dados não sejam alterados por entidades não autorizadas;

- Confidencialidade: necessidade de proteger informações sensíveis de forma a não serem vistas indiscriminadamente;
- Disponibilidade: disponibilidade de acesso ao sistema para usuários autorizados;
- Autenticação: processo pelo qual a identidade de uma pessoa possa ser verificada;
- Autorização: associar uma identidade a uma lista de direitos, privilégios, ou áreas de acesso;
- Não repudiação (ou Legalidade): quando alguém não pode negar a autenticidade de um documento, a sua assinatura ou o seu envio;
- Auditoria: processo de assegurar que a atividade de um usuário possa ser devidamente registrada e revista para detectar eventos suspeitos.

E também pelos mecanismos que objetivam a segurança dos PEP como:

- Controle de acesso por *login* e Senha: a autenticação inclui a validação de senha do usuário, proibição de acesso a usuários suspensos, solicitação automática de mudança de senha caso esteja expirada, bloqueio de usuários que excederam o número (configurado) de tentativas de acesso sem sucesso, utilização de um número mínimo de caracteres para a senha, etc.
- Certificados Digitais: São documentos eletrônicos que utilizam duas chaves, uma pública de conhecimento geral, e outra privada, que deve ser mantida em sigilo pelo titular do certificado.
- Biometria: é a ciência que estuda a identificação baseada na medição de traços biológicos, através de: reconhecimento de voz e de íris, verificação de assinatura manuscrita, reconhecimento da geometria da mão, reconhecimento de impressão digital, reconhecimento de face, reconhecimento da dinâmica de digitação, etc.
- *Firewall*: (parede de fogo): com um *firewall* pode-se filtrar o que se desejar que saia ou entre numa determinada rede; funciona como um sistema que controla e permite acesso de fora para dentro e vice-versa, somente a usuários autorizados evitando acessos indevidos, mesmo que estes acessos sejam internos da rede.
- Políticas e Práticas: liberar ou bloquear o acesso ao PEP – ao mesmo tempo que a informação deve estar segura, ela também não deve sofrer restrições excessivas de acesso que possam comprometer a utilização legítima do sistema.
- *Backups* e *Log* de auditoria: *backup* dos dados ou arquivos são feitos normalmente em fitas, discos rígidos externos ou mesmo disquetes. Os registros de *Log* funcionam como um histórico de acessos a um determinado servidor de arquivos ou a um único arquivo. Os *Logs* de Auditoria são as análises periódicas sobre estes arquivos com o intuito de fiscalizar acessos indevidos ou atividades que comprometam a integridade dos dados ou do próprio servidor.

Porém para se alcançar todas as vantagens do Prontuário Eletrônico do Paciente, ainda há que se solucionar muitos dos problemas éticos, legais e técnicos (MARTINS, 2004).

Em relação ao vazamento de informações é muito comum vermos na mídia informações médicas sobre famosos, e assim surge um questionamento sobre os limites entre sensacionalismo e informação, como exemplo Fortes (2000) cita o governador de São Paulo Mário Covas que possuía um tumor maligno, seus médicos realizaram declarações minuciosas na mídia e ainda detalharam com imagens, isso tudo porque políticos tem um compromisso de exercer sua função pública e caso algo impeça isto é permitido retratar-se com a população, entretanto este retratar-se poderia se resumir numa declaração médica que o governador estava afastado do cargo por questões médicas.

É evidente que os meios de comunicação se utilizam de informações restritas de pessoas públicas para ganharem audiência expondo estas sem medir o sofrimento que estão passando, por isso é preciso atentar sobre as questões de privacidade de todos os pacientes.

Por isso, segundo Fortes (2000 p. 320) “percebe-se a necessidade urgente do estabelecimento de práticas no âmbito da saúde que potencializem a autonomia dos cidadãos e os protejam de possíveis abusos que firam suas dignidades”.

Sendo a confidencialidade fortemente vinculante, mas não uma obrigação absoluta, a questão ética que se impõe é a de determinar quais princípios ou circunstâncias justificam a ruptura do sigilo, o que baseia-se no princípio de Justiça e depende do contexto particular de cada caso. Essas circunstâncias estão relacionadas com a segurança de terceiras partes conhecidas – princípio da não maleficência -, com a preocupação ao bem-estar público e social – princípio da beneficência -, com o respeito da autonomia do paciente e se a informação pode ser utilizada em situações com características idênticas – contemplando o princípio da justiça (LOCH, 2006).

Diante disso, explicitar as situações que demandam a ruptura da confidencialidade e discuti-las com o paciente pode ser uma forma moralmente correta de evitar a decepção e a diminuição da confiança mútua. Além disso, é fundamental que se estabeleçam políticas prudentes e eticamente adequadas para regular estas questões. O objetivo principal deve pairar entre a proteção da privacidade individual e a garantia de um rápido fluxo de informações para os profissionais de saúde que legitimamente dela necessitam (LOCH, 2006).

3. METODOLOGIA

A metodologia utilizada neste trabalho tem caráter teórico-reflexivo e está baseada em pesquisas bibliográficas a livros, teses de doutorado, dissertações de mestrado, artigos, apresentações e sites, com especial foco nas questões bioéticas e de segurança e confidencialidade na informação do paciente. Além de como esses dados devem ser mantidos sigilosos pelas instituições e todos os profissionais da área de saúde que tem acesso aos mesmos.

4. ANÁLISES E DISCUSSÕES

A partir da metodologia aplicada foi possível elaborar o presente artigo bem como as reflexões acerca das questões éticas envolvidas. Assim temos como resultado uma visão sobre o uso ético dos Prontuários Eletrônicos do Paciente a partir do referencial teórico que se segue. Tal referencial encontra-se elencado nos conceitos de Prontuário do Paciente, vantagens e desvantagens do PEP, aspectos e princípios de segurança, e os aspectos éticos e legais envolvidos, salientando que os padrões morais não podem em hipótese alguma sobressair-se aos éticos quando a saúde é o objetivo em questão.

5. CONSIDERAÇÕES FINAIS

O uso crescente de tecnologias nos Sistemas de Saúde cria novas formas de se romper a confidencialidade do paciente. Não é que esta quebra não ocorra sem a tecnologia, mas que é facilitada, isso não há dúvidas. Por isso, os hospitais precisam criar normas para impedir este problema, como por exemplo, instalar sistemas que exijam a senha e *login* tanto do profissional, quanto do paciente, além de outros sistemas como biometria, *firewall*, políticas e normas de segurança, certificados digitais, *backup* e *log*, entre outros recursos. Ou também, pode-se utilizar os 50 mecanismos de privacidade de informação segundo Magnagnagno (2015). Há sim formas simples e eficazes de impedir o amplo acesso aos dados do usuário. Cumpre salientar que faz-se necessário que os profissionais que irão lidar com os meios tecnológicos saibam realizar o armazenamento adequado das informações do paciente, pois tal anotação é o meio legal que comprova o que foi de fato realizado neste.

Outras normas que podem ser evidenciadas são as questões éticas da equipe de saúde, pois o vazamento de informações pode causar muitos danos aos pacientes, principalmente se estas forem informações genéticas, já que muitas vezes não estão relacionadas a apenas uma pessoa, mas aos seus ascendentes e descendentes também. Além dessas informações também estão contidos dados sobre as características físicas e psicológicas do portador, hábitos sociais e familiares, resumindo, toda a história de vida pregressa do paciente, que se reveladas podem acarretar os mais variados prejuízos. O profissional tem o dever de evitar causar estes tipos de danos.

É imprescindível reconhecer que todas as pessoas independentemente da sua condição, capacidade ou idade, possuem dignidade e por isso precisamos respeitar sua decisão de não querer que suas informações sejam transmitidas. É preciso sabedoria para agir diariamente com ética, pois um erro pode causar vários impasses. Assim é necessária a total colaboração das instituições e dos funcionários que tem acesso aos dados dessas pessoas, para que essas informações, que são exclusivamente reveladas em confidencialidade mediante a confiança estabelecida pela relação médico-paciente, sejam mantidas em sigilo para garantir essa dignidade e também a permanência da confiabilidade.

Toda essa Revolução na Informática pode destrinchar e agilizar melhorias no atendimento e no apoio ao enfermo, assim, se ela for normatizada de um modo onde a privacidade do usuário permaneça íntegra, ou seja, de uma forma onde a informação seja uma propriedade do paciente e onde os hospitais e clínicas possuam não só apenas a guarda desta, mas juntamente a responsabilidade do sigilo, haverá benefícios visto que a agilidade, a eficiência e a qualidade aumentarão, assim como os erros diminuirão.

A área da saúde e informação estão se relacionando cada vez mais, como exemplo temos cada vez mais cirurgias realizadas por vídeo, auxílio de robôs, entre outros mecanismos de auxílio para facilitar interações que visem a melhora do paciente. Basta associar o uso ético destas informações que o caminho para uma medicina cada vez mais solícita e de qualidade progredirá.

REFERÊNCIAS

ANS - AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. A agência reguladora dos planos de saúde do Brasil. Folder institucional, dezembro 2012.

BRASIL, Decreto-Lei No 2.848, de 7 de dezembro de 1940. Código Penal Presidência da República.

_____. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF, Senado, 1998.

BRASIL, Decreto-Lei No 2.848, de 7 de Dezembro de 1940. Código Penal Presidência da República.

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

CRM - CONSELHO FEDERAL DE MEDICINA. Manual de Orientação Ética e Disciplinar. Vol. 1 - 2a. edição. Florianópolis-SC, 2000

COSTA, C. G. A. da. Prontuário Eletrônico do Paciente: Legislação, Auditoria e Conectividade. In: **8º Congresso Latino Americano de Serviços de Saúde**, Marília, SP, 2003.

FORTES, P. A. C.; ANJOS, M. F. Desafios para a preservação da privacidade no contexto da saúde. In: **Revista Bioética**, 2000.

FRANCISCONI, C.F.; GOLDIM, J.R. Aspectos bioéticos da confidencialidade e privacidade. In: **Revista Iniciação à Bioética**. Brasília: Conselho Federal de Medicina, 1998.

GAERTNER, A.; SILVA, H. P. da. **Privacidade de informação na internet: ausência de normalização**, Bahia, 2005.

GOLDIM, J. R.; FRANCISCONI, C. F. Bioética e Informação. Disponível em <<http://www.bioetica.ufrgs.br/bioinfo.htm>> Acesso em 10 set 2015. Bioética. Porto Alegre, Brasil, 1998.

GOSTIN, L.O.; TUREK-BREZINA. J.; POWERS, M.; KOSLOFF, R.; FADEN, R.; STEINAUER, D.D. Privacy and security of personal information in a new health care system. **Jama**. 1993;270:2487-93.

GRISARD, N. Manual de Orientação Médica e Disciplinar. Disponível em <http://www.portalmedico.org.br/Regional/crmse/manual/sumario.htm> Acesso em: 06 out. 2015.

LOCH, J. de A. Confidencialidade: natureza, características e limitações no contexto da relação clínica. In: **Programa de Pós-Graduação em Medicina e Odontologia**, PUCRS, RS, 2006.

MAGNAGNAGNO, O. A. **Mecanismos de proteção da privacidade das informações do prontuário eletrônico de pacientes de instituições de saúde**. 31/03/2015. 138 f. Dissertação (Mestrado em Administração) - Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul, 2015.

MARTINS, A.; SAUKAS, E.; ZANARDO, J. SCAI: Sistema de controle de acesso para os requisitos da saúde. In: **Anais do IX Congresso Brasileiro de Informática em Saúde**, Ribeirão Preto, SP, 2004.

MIRABETE, J. F; FABRINNI, R. N. **Código Penal Interpretado**. 8 ed. Ed. Atlas, São Paulo, 2013.

MOTTA, G. H. M. B. Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos. In: **Tese de Doutorado, Escola Politécnica da USP**, São Paulo, SP, 2003.

SALVADOR, V. F. M.; ALMEIDA FILHO, F. G. V. de. Aspectos éticos e de segurança do prontuário eletrônico do paciente. In: **II Jornada do Conhecimento e da Tecnologia**, UNIVEM, Marília, SP, 2005.

SIMIONATO, A. C.; SANTANA, R. C. G.; SANTOS, P. L. V. A. da C. Privacidade e os simulacros digitais gerados pelos dados pessoais. In: **Encontro Internacional Dados, Tecnologia e Informação**, Marília, SP, 2013.

SOARES, N. V; DALL'AGNOL, C. M. Privacidade dos pacientes – Uma questão ética para a gerência do cuidado em enfermagem. In: **Acta Paul Enferm**, Santo Ângelo, RS, 2011.