MINUTA

RESOLUÇÃO CIT Nº XXXX, DE XX DE XXX DE 2018

Dispõe sobre a proteção e tratamento de dados pessoais em saúde e estabelece procedimentos para acesso à informação e cessão de bases de dados contendo informações pessoais custodiadas pelo SUS.

A COMISSÃO INTERGESTORES TRIPARTITE, no uso das atribuições que lhe conferem o inciso I do art. 14-A da Lei nº 8.080, de 19 de setembro de 1990, e tendo em vista o disposto no inciso I do art. 32 do Decreto nº 7.508, de 28 de junho de 2011, e

Considerando a Constituição Federal, que dispõe em seu art. 196 sobre a garantia da saúde mediante políticas sociais e econômicas que visem à redução do risco de doença;

Considerando a Lei nº 8.080, no seu Art. 3º, de 19 de setembro de 1990, que dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências;

Considerando a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

Considerando a Lei n° 8.429, de 2 de junho de 1992, que dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências;

Considerando a Lei nº 9.278, de 10 de maio de 1996, que regula o § 3º do art. 226 da Constituição Federal;

Considerando a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111,

de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

Considerando a importância de garantia da privacidade para assegurar a confiança da população na guarda de seus dados individuais de saúde pelo Sistema Único de Saúde (SUS), e

Considerando que o acervo de dados existentes relacionados à assistência, promoção, prevenção e à vigilância relacionados à saúde da população brasileira constitui-se em imprescindível fonte de informações para pesquisas e para a gestão da saúde no país e que seu uso socialmente responsável é de relevante interesse público, cuja não utilização gera questionamentos de natureza ética, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º. Esta resolução dispõe sobre a proteção e tratamento de dados pessoais em saúde e estabelece procedimentos para acesso à informação e cessão de bases de dados contendo informações pessoais custodiadas pelo SUS.

Excluído: Dispor

Excluído: r

Art. 2º. Para efeito desta Resolução, considera-se:

I - acesso a base de dados: estabelecimento de conexão, entre um indivíduo ou entidade, e um sistema de comunicação ou de informação, na qual pode ocorrer transferência de dados e ativação de processos computacionais, não havendo, necessariamente, cessão de base de dados;

II - agente público legalmente autorizado: todo aquele que exerce, nas três esferas de gestão do SUS, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na administração pública e que possui condição pessoal – inerente ao efetivo exercício de cargo, função, emprego ou atividade – indispensável para o acesso ou cessão das bases de bancos de dados com informações pessoais em saúde. São todos aqueles diretamente envolvidos na assistência à saúde do indivíduo, ou vinculados a órgãos ou entes que realizam atividades típicas de Estado na área de saúde, a exemplo daquelas desenvolvidas nas ações de vigilância em saúde, auditoria em saúde, pesquisa e avaliação em saúde, gestão de sistemas de informação e gestão de custódia de dados;

Excluído: bem como os

III – ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação, bem como locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV – banco ou base de dados: ativo de informação ou repositório de dados relacionados a um determinado assunto e armazenados em um dispositivo eletrônico, organizados de forma a permitir a criação, atualização, ou a recuperação mais eficiente de informação;

V – base de dados contendo informações pessoais em saúde: repositório de dados com informações que devem ser protegidas para a preservação dos direitos individuais previstos nos incisos X, XII e XIV do art. 5º da Constituição Federal e na Lei nº 12.527, de 2011;

Excluído: 2

VI – cessão de base de dados: processo de disponibilização de cópia total ou parcial de base de dados, ou arquivos de disseminação com representação dos dados contidos nestas bases;

VII– concedente: área responsável pela permissão de acesso, pela cessão de bases de dados ou de informações nelas contidas;

VIII – consentimento: manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais em saúde para uma finalidade determinada;

IX – contas de serviço: contas de acesso à rede corporativa de computadores, necessárias a um procedimento automático sem qualquer intervenção humana no seu uso;

X – custodiante: órgão, entidade ou unidade com capacidade técnica e responsabilidade formal para prover armazenamento, transporte, operação, administração, segurança e preservação de ativos de informação que não lhe pertençam, mas que estejam sob sua custódia, sendo responsável por aplicar os níveis de controles de segurança em conformidade com as exigências da segurança de informação e comunicações;

XI – dado: elemento que compõe a informação, preparado para ser processado, operado e transmitido por um sistema ou programa de computador;

XII – dados desidentificados: conjunto de dados que não permita a identificação da pessoa por meio do uso de técnicas de tratamento de dados;

Excluído: suficientemente seguro para impedir

XIII – dados pessoais: representação de fatos, juízos ou situações referentes a uma pessoa física, passível de ser captada, armazenada, processada ou transmitida, por meios informatizados ou não, que permitam a identificação da pessoa ou possam ser associados a outros dados referentes ao endereço, idade, raça, opiniões políticas, religiosas, crenças, ideologia, saúde física, saúde

mental, vida sexual, registros policiais, assuntos familiares, assuntos da intimidade e da vida privada, profissão e outros que a Lei assim o definir, devendo ser protegidas para a preservação dos direitos individuais previstos nos incisos X, XII e XIV, do art. 5º, da Constituição Federal, e na Lei nº 12.527, de 2011;

XIV – desidentificação de dados pessoais: processo de retirar ou modificar os dados de modo a impossibilitar ou dificultar a identificação, de forma direta ou indireta, da pessoa, com o mínimo de perda de informação, sendo que, em dados de saúde, o nome, endereço e código postal, além de outros que conjuntamente possam identificar o paciente ou gerar tratamento discriminatório, devem ser modificados ou retirados;

XV – entidades vinculadas: são aquelas citadas no Decreto nº 8901 de 10 de novembro de 2016 ou outro normativo que venha a atualizá-lo.

XVI – eventos de saúde: ocorrência identificada, no âmbito do SUS, que exija tratamento ou execução de procedimentos por um de seus profissionais;

XVII – gestor da informação: agente responsável pela gestão de um determinado sistema de informação, a quem cabe entre outras responsabilidades o gerenciamento das permissões de acessos aos dados destes sistemas;

XVIII – gestor de custódia: pessoa física nomeada pelo Custodiante de um ativo de informação, com a responsabilidade da gestão dos procedimentos necessários para o adequado desempenho das competências do Custodiante relativas ao referido ativo de informação;

X –

XIX– informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XX – informação pessoal: informação relacionada a pessoa natural identificada ou identificável, cujo acesso possui caráter restrito;

XXI - informação pessoal em saúde: informação pessoal que trata acerca das condições de saúde do indivíduo e de suas relações com os serviços assistenciais de saúde;

XXII – sistema consumidor: sistema de informação que consome dados gerenciados por outros sistemas de informação;

[CAP1] Comentário: Substituído termo indivíduo por titular. Ver inciso XXVI

Excluído: VIII

Excluído: indivíduo

Excluído: : pessoa natural a quem se referem os dados pessoais em saúde objeto de tratamento;

XXIII – sistema de informação: sistema de coleta, armazenamento, processamento e disponibilização de dados referentes a um ou mais temas, associado a um banco de dados e utilizado na organização de atividades do SUS, no suporte aos profissionais de saúde e na disponibilização autorizada de informações;

XXIV – sistema fornecedor: sistema de informação que fornece dados para consumo a outros sistemas de informação;

XXV – solicitante: pessoa física ou jurídica que faz solicitação de acesso a base de dados ou informações nela contidas;

XXVI - Titular: pessoa natural a quem se referem os dados e informações pessoais em saúde objeto de tratamento;

XXVII – tratamento da informação: conjunto de ações referentes à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

XXVIII– unidade de vinculação ou relacionamento de dados: estrutura organizacional responsável pela vinculação ou relacionamento (“linkage”) de dados, sendo designada como unidade descentralizada de relacionamento de dados se for externa ao Ministério da Saúde, e às Secretarias de Saúde dos Estados, Municípios e Distrito Federal;

XXIX – vinculação ou relacionamento de dados (“data linkage”) pessoais: processo de vincular ou relacionar dados pertencentes a uma mesma pessoa, mesmo quando não identificada ou identificável, contidos em bases de dados de natureza diversa, de forma a compor registros longitudinais de saúde dos indivíduos e correlacionar fatores distintos associados a eventos de saúde, sendo condição necessária para realização de pesquisas na área de saúde;

Excluído: VIII

XXX - Unidades de Integração de Dados (UID) para Pesquisa Científica e Tecnológica e Avaliação em Saúde: instituições públicas que possuam dentre as suas funções a pesquisa e avaliação em saúde e que sejam dotadas de infraestrutra para tratamento de grande bases de dados pessoais de interesse público para a realização de pesquisa cientifica, tecnológica e de avaliação em saúde, realizando procedimentos de vinculação ou relacionamento de dados, e garantindo níveis de segurança da informação e proteção de dados pessoais compatíveis com as normas técnicas e boas práticas de segurança da informação;

Excluído: I

XXXI - Curadoria de dados: conjunto de procedimentos utilizados para o gerenciamento do ciclo de vida das informações coletadas e processadas, com a finalidade de garantir sua coleta, seleção, qualidade, memória, arquivamento, integridade, preservação e acesso.

CAPÍTULO II
DOS PRINCÍPIOS GERAIS DE PROTEÇÃO DE DADOS PESSOAIS EM SAÚDE

Art. 3º. As atividades de tratamento de dados pessoais em saúde deverão atender aos seguintes princípios gerais:

I - princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas e explícitas ao titular das informações pessoais;

II - princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades almejadas e com as legítimas expectativas do titular das informações pessoais, de acordo com o contexto do tratamento;

III - princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;

IV – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

V – princípio da segurança, pelo qual devem ser adotadas medidas técnicas e administrativas de segurança capazes de prevenir a ocorrência de acesso e divulgação indevidos durante o processo de tratamento de dados pessoais em saúde;

Excluído: .

VI – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.

CAPÍTULO III
DA PROTEÇÃO E TRATAMENTO DOS DADOS PESSOAIS EM SAÚDE

Art. 4º. As informações pessoais em saúde devem ser protegidas e custodiadas pelas instâncias gestoras do SUS, no âmbito de suas competências, e:

I – terão seu acesso restrito ao titular e aos agentes públicos legalmente autorizados para o exercício de suas funções;

II - poderão ter sua divulgação e acesso por terceiros autorizados por previsão legal ou consentimento expresso do titular.

Excluído: indivíduo

§1º. Todos os que se envolverem no tratamento dos dados, inclusive os agentes públicos legalmente autorizados, devem atender aos princípios gerais previstos no Capítulo II.

Art. 5º. O consentimento referido no inciso II do art. 4º não será exigido quando o acesso à informação pessoal em saúde for necessário:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, vedada a identificação da pessoa a que a informação se referir;

III - ao cumprimento de decisão judicial;

IV - à defesa de direitos humanos; ou

V – à proteção do interesse público e geral preponderante.

Paragrafo Único. Os dados devem ser tratados exclusivamente para as finalidades previstas nos incisos, conforme os princípios gerais previstos no Capítulo II, garantidos os direitos do indivíduo.

Art. 6°. O tratamento dos dados pessoais em saúde deve ser realizado de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem dos indivíduos, tendo como finalidade a saúde dos indivíduos e da população, através da assistência, prevenção, promoção, pesquisas, avaliações e formulações de políticas públicas.

CAPÍTULO IV
DOS GESTORES DA INFORMAÇÃO E CUSTODIANTES

Art. 7º. No âmbito do Ministério da Saúde serão designados Gestores da Informação, e seus respectivos suplentes, para a gestão do conjunto de sistemas de informação nacionais vigentes.

§ 1º O titular da Secretaria será o gestor da informação e responsável pela gestão dos respectivos sistemas, a quem caberá, ainda, designar seu suplente.

§ 2º O titular da Secretaria de que trata o §1º poderá delegar a competência de Gestor da Informação a titular de órgão integrante da estrutura de sua Secretaria ou a servidor público sob sua chefia imediata.

Art. 8º. No âmbito dos Estados, do Distrito Federal e dos Municípios, o titular da Secretaria de Saúde será o Gestor da Informação, dos sistemas de informação sob sua jurisdição, a quem caberá ainda designar seu suplente.

Parágrafo único. O titular da Secretaria de Saúde de que trata o caput poderá delegar a competência de Gestor da Informação a titular de órgão integrante da estrutura de sua Secretaria ou a servidor público sob sua chefia imediata.

Art.9º. No âmbito das Entidades Vinculadas, o dirigente será o Gestor da Informação em relação aos sistemas de informação sob sua jurisdição, a quem caberá designar seu suplente.

Parágrafo único. A Entidade Vinculada poderá delegar a competência de Gestor da Informação a titular de órgão ou unidade integrante da estrutura de sua Entidade ou a servidor público sob sua chefia imediata.

Art. 10. O Departamento de Informática do SUS (Datasus) será o Custodiante dos bancos de dados hospedados nas instalações do Ministério da Saúde.

§1° Nos Estados, no Distrito Federal e nos Municípios, o titular da Secretaria de Saúde designará o Custodiante dos bancos de dados no âmbito da sua competência.

§2° Nas entidades vinculadas ao Ministério da Saúde, o dirigente principal da entidade designará o custodiante dos bancos de dados no âmbito de sua competência.

§3° O Custodiante definirá 1 (um) Gestor de Custódia, titular e suplente, para cada base de dados sob sua tutela, podendo essa definição ser vinculada a cargos da estrutura interna da instituição.

CAPÍTULO V
DA VINCULAÇÃO E DESIDENTIFICAÇÃO DE DADOS PESSOAIS EM SAÚDE

Art. 11 . No âmbito do Ministério da Saúde, o Datasus, por meio de sistema informatizado, sempre que necessário para evitar a exposição de dados pessoais em saúde, realizará a atividade de vinculação e desidentificação de dados nos casos de cessão de informações presentes em bases de dados distintas.

Parágrafo único. Os gestores dos Estados, Distrito Federal e Municípios, e as entidades vinculadas, no âmbito de suas competências, poderão definir unidades de vinculação de dados mantidas no seu ambiente de custódia.

Art. 12. Os dados resultantes de processos de vinculação devem ser desidentificados antes de sua cessão ou divulgação.

§ 1º Os produtos resultantes do processo de vinculação e desidentificação de dados e a documentação do método empregado serão disponibilizados aos respectivos Gestores da Informação, para os devidos fins, em conformidade com os princípios descritos no Capítulo II desta Resolução.

§ 2º Os Gestores da Informação de cada sistema de informação deverão manter e divulgar uma lista com os produtos resultantes do processo de vinculação contendo informações sobre suas principais características, tais como: fontes de dados originais, período de referência, abrangência territorial, método empregado na vinculação, respectivas limitações, dentre outros.

§ 3º A metodologia utilizada pelo Custodiante na vinculação e/ou desidentificação de dados deverá ser validada pelos Gestores da Informação responsáveis pelos sistemas de informação envolvidos.

CAPÍTULO VI
DAS UNIDADES DE INTEGRAÇÃO DE DADOS (UID) PARA PESQUISA CIENTÍFICA E TECNOLÓGICA E AVALIAÇÃO EM SAÚDE

Art. 13. As instituições de pesquisa, ciência, tecnologia e inovação públicas, que não apresentem conflitos de interesse com a natureza dos dados de saúde, são aptas a requerer ao Ministério da Saúde seu credenciamento como Unidades de Integração de Dados (UID) para Pesquisa Científica e Tecnológica e Avaliação em Saúde ao Ministério da Saúde.

§1º O credenciamento de que trata o caput será submetido à aprovação do Comitê Gestor da Estratégia e-Saúde.

§2°. O credenciamento referido no caput será condicionado à comprovação de competência técnica para proteger e tratar dados pessoais em saúde, que será demonstrado por:

I - atendimento aos critérios estabelecidos de proteção de dados e segurança da informação.

II - possuir responsável técnico pela documentação do uso do dados.

III - possuir governança adequada para as funções a serem desempenhadas.

IV - prever a utilização dos dados decorrentes da cessão exclusivamente para finalidades de reconhecido interesse público, sem fins comerciais.

§3°. As normas, processos e critérios adotados para o credenciamento de que trata o caput serão recomendados pelo Comitê de Informação e Informática em Saúde, por intermédio do Subcomitê Gestor de Segurança da Informação e Comunicação (SGSIC/CIINFO/MS).

§4º O credenciamento será concedido por período de 5 anos, ao final do qual poderá ser renovado por sucessivos e iguais periodos.

§5º O não cumprimento das normas estabelecidas no credenciamento poderá levar ao seu descredenciamento a qualquer tempo.

§6º As Unidades de Integração de Dados para Pesquisa Científica e Tecnológica e Avaliação em Saúde (UID) tornam-se custodiantes dos dados cedidos durante o período do credenciamento.

[CAP2] Comentário: Repetido parágrafo 1º.

Excluído: §4º O credenciamento de que trata o caput será submetido à aprovação do Comitê Gestor da Estratégia e-Saúde

Excluído: . ¶

Excluído: 5

Excluído: ao final do qual poderá ser renovado,

Excluído: 6

Excluído: 7

Art. 14. As Unidades de Integração de Dados (UID) têm por finalidade:

I - realizar a curadoria dos dados;

II - integrar base de dados da saúde de naturezas diversas entre si e com outras bases de dados estatísticas, administrativas e de pesquisas para ampliar o conhecimento em saúde;

III - realizar pesquisa cientifica, tecnológica e de avaliação em saúde;

IV - apoiar o Ministério da Saúde, Secretarias Estaduais de Saúde e Secretarias Municipais de Saúde na formulação e avaliação de políticas públicas para o SUS.

§1º. As Unidades de Integração de Dados (UID) não poderão compartilhar dados pessoais com outras instituições e nem utilizá-los para natureza diversa a suas finalidades.

Art. 15. Os produtos resultantes do processo de integração de dados realizado pelas Unidades de Integração de Dados (UID) poderão ser solicitados pelo Ministério da Saúde, pelas Secretarias Estaduais de Saúde e Secretarias Municipais de Saúde, que poderão utilizá-los ou cedê-los a terceiros.

§1º. As Unidades de Integração de Dados (UID) poderão disponibilizar dados desidentificados, produto da integração, a pesquisadores vinculados à instituições públicas, que tenham entre as suas missões a pesquisa, cujos projetos possuam parecer favorável emitido pelo Sistema CEP/CONEP.

§ 2º. As Unidades de Integração de Dados (UID) deverão informar periodicamente ao gestor da base de dados as solicitações atendidas de que trata o parágrafo anterior.

§3º. Os pesquisadores deverão assinar termo de responsabilidade para recebimento dos dados desidentificados em conformidade com os princípios gerais de proteção de dados descritos no Capitulo II.

Art. 16. As Unidades de Integração de Dados (UID) poderão solicitar a cessão a qualquer tempo de base de dados contendo informações pessoais em saúde custodiadas pelo SUS mediante sua especificação, de forma clara e precisa, cabendo a cessão ser avaliada pelo respectivo gestor.

Parágrafo único: A cessão dos dados nominais completos dos sistemas de informação de saúde custodiados pelo Ministério da Saúde para as Unidades de Integração de Dados (UID) será realizada de forma contínua durante o período em que vigir o seu credenciamento, mediante atualização dos termos de responsabilidade.

CAPÍTULO VII
DA SOLICITAÇÃO DE ACESSO OU DE CESSÃO DE BASE DE DADOS DO SUS

Art. 17. A solicitação de acesso ou de cessão de qualquer base de dados contendo informações pessoais em saúde custodiadas pelo SUS deve ser formalizada mediante o preenchimento obrigatório dos formulários de “solicitação de acesso ou de cessão das bases de dados que contenham informações pessoais custodiadas pelo SUS” (anexo A), bem como do “termo de responsabilidade e confidencialidade” (anexo B), que disporá sobre a finalidade e a destinação de uso das informações solicitadas, sobre as obrigações a que se submeterá o requerente e sobre

seu compromisso de garantir a privacidade e confidencialidade dos dados objeto do pedido de acesso ou cessão.

§ 1º O formulário de solicitação de acesso ou de cessão (anexo A) conterá, imprescindivelmente as seguintes informações:

Excluído: ao menos

I - nome do requerente e identificação da instituição a que representa, quando couber;

II - número de documento de identificação válido;

III - especificação, de forma clara e precisa, da base de dados cujo acesso ou cessão é requerido, juntamente com o período de abrangência;

IV - endereço físico e eletrônico do requerente, para recebimento de comunicações ou do produto requerido;

V - informações que caracterizem o enquadramento do solicitante nas condições de:

a) titular da informação e/ou;

b) agente público autorizado e/ou;

c) portador de termos de consentimento para acesso à informação solicitada e/ou;

d) portador de documentação que caracterize as dispensas de consentimento previstas na legislação, reproduzidos no artigo 5º desta Resolução e/ou;

e) portador de documentação que comprove o interesse pela recuperação de fatos históricos de maior relevância, observados os procedimentos previstos no art. 34 da Portaria GM-MS nº 1.583 de 2012.

§ 2° À solicitação de informação pessoal de que trata o inciso I do art. 5° deve constar laudo médico que comprove a incapacidade física ou legal da pessoa cuja informação se referir, bem como exposição de motivos que demonstre a justa finalidade de utilização das informações para tratamento médico.

§ 3° Quando a solicitação se enquadrar no inciso III do art. 5°, o formulário de solicitação de acesso ou cessão será preenchido pelo gestor da informação e encaminhado ao custodiante, acompanhado da Ordem Judicial em questão.

§ 4º Solicitações provenientes de instituições que desenvolvem pesquisa científica, devem ser acompanhadas de parecer favorável do sistema CEP/CONEP em conformidade com as Resoluções vigentes, mencionando expressamente que a pesquisa fará uso das bases de dados de sistemas de informação cujo acesso ou cessão é requerido.

§ 5º Solicitações provenientes de secretarias de saúde municipais, estaduais e do Distrito Federal, que envolvam dados de eventos em saúde que extrapolam a residência ou ocorrência de sua jurisdição, devem ser acompanhadas de justificativa.

§ 6º O solicitante deve atestar que dispõe de condições de armazenar com segurança os dados contendo informações pessoais, descrevendo seu ambiente computacional e as medidas de segurança adotadas, conforme especifica o Decreto n° 7.845, de 14 de novembro de 2012, colocando o seu ambiente físico e virtual à disposição do Ministério da Saúde para que este possa proceder, caso julgue necessário, à auditoria, à vistoria e à comprovação da existência das condições de segurança necessárias.

§ 7º O Datasus deverá garantir, por meio de um processo informatizado e transparente, o processo de solicitação e aprovação de acessos e cessões de base de dados sob sua custódia, de forma garantir a informação ao solicitante, desde que autorizado pelo gestor da informação ou por autoridade superior que tenha competência para fornecer tal autorização.

CAPÍTULO VIII
DA ANÁLISE E AUTORIZAÇÃO DAS SOLICITAÇÕES

Art. 18. As solicitações de acesso ou cessão de bases de dados contendo informações pessoais serão avaliadas pelo(s) Gestor(es) da Informação da(s) base(s) de dados solicitada(s), que fará, em primeira instância, avaliação sobre a relevância e admissibilidade do pedido, conforme o previsto no art. 17

§ 1º Os critérios para que se proceda a avaliação de que trata o caput serão a adesão da solicitação aos princípios gerais de proteção de dados pessoais em saúde, previstos nos incisos I, II e III do art. 3°.

§2° Se a avaliação de que trata o “caput” for negativa, o Gestor da Informação Competente cientificará o Solicitante com a devida justificativa.

§3° Produtos de vinculação de dados, quando desidentificados, podem, após avaliação dos respectivos Gestores da Informação, ser disponibilizados para transparência ativa, nos termos da Lei 12.527 de 2012.

Art. 19. Caso a avaliação de que trata o “caput” do art. 18 seja positiva, o Gestor da Informação a encaminhará ao Custodiante que fará parecer avaliativo sobre,:

I - a possibilidade de o atendimento à solicitação acarretar algum risco para a segurança da informação e comunicação em saúde;

II - a possibilidade de se proceder à desidentificação das informações solicitadas e o prazo para a referida disponibilização;

III - a possibilidade de se proceder à vinculação das informações solicitadas e o prazo para a referida disponibilização.

Art. 20. O parecer do Custodiante atenderá à solicitação avaliada como positiva pelo Gestor da Informação, com exceção das seguintes situações:

I – Quando o acesso ou cessão de bases de dados represente real e justificado risco à segurança da informação e comunicação em saúde e à estabilidade dos sistemas de informação ou ao ambiente de bancos de dados; ou

II – Quando as solicitações forem genéricas, desarrazoadas, desproporcionais ou que exijam trabalhos adicionais de análise, interpretação ou consolidação de dados e informações ou serviços de produção ou tratamento de dados que não estejam dentro da competência do Custodiante.

Art. 21 O Custodiante encaminhará o parecer avaliativo ao Gestor da Informação, o qual decidirá sobre a possibilidade ou não de atendimento da solicitação:

§1° Caso seja negada a solicitação, o Gestor da Informação comunicará ao solicitante, via sistema, sobre a possibilidade de interposição de recurso junto à instância referida no art. 26.

§2° É vinculante ao Gestor da Informação a avaliação negativa do Custodiante com base na existência de risco à segurança da informação e comunicação em saúde.

Art. 22. Quando a solicitação se enquadrar nos incisos I e III do art. 5°, o acesso ou cessão será concedido pelo Gestor da Informação sem necessidade de encaminhamento ao Custodiante.

Art. 23. As solicitações de acesso ou cessão de bases de dados contendo informações pessoais oriundas de atores internos do Ministério da Saúde passarão pela mesma tramitação de que trata esta Resolução.

Art. 24. No âmbito do Ministério da Saúde, o Gestor da Informação pode indicar nominalmente agentes públicos autorizados a acessar de modo contínuo os dados nominais completos dos sistemas de informação sob sua gestão, armazenados no ambiente do Custodiante.

§ 1º O acesso aos dados completos, nos termos do "caput", se justificará quando a área técnica do Ministério da Saúde realizar atividades de monitoramento de regularidade na produção de dados, análise de consistência, tratamento dos dados, validação e preparação de dados para disseminação.

§ 2º O acesso, quando autorizado, será concedido e renovado, se necessário, por período não superior a seis meses, pelo Gestor de Custódia, mediante normas regulamentadoras praticadas pela instituição.

§ 3º O agente público autorizado que tiver acesso contínuo às bases de dados, nos termos do "caput" e do §1º, poderá armazenar arquivos com extrato de dados da base sob sua gestão, no recurso computacional de sua estação de trabalho, desde que use criptografia nas pastas onde os dados venham a ser armazenados.

Art. 25. Quando a solicitação tiver como objetivo a alimentação de outros sistemas de informação, o acesso a um banco de dados só será permitido se expressamente autorizado pelo respectivo Custodiante e Gestor da Informação do sistema fornecedor, sendo que o sistema consumidor desses dados somente terá acesso automático aos dados por meio de contas de serviços, sendo vedada sua replicação para outro ambiente sem a devida autorização.

Art. 26. O CIINFO/MS, no âmbito do Ministério da Saúde, é a autoridade competente para análise de recursos em última instância, quanto às solicitações de acesso ou cessão de banco de dados contendo informações pessoais que se enquadrem nas situações mencionadas nos incisos II, IV e V do art. 5º, associadas às circunstâncias em que o Gestor da Informação ou o Custodiante declarar que não há possibilidade de acesso ou cessão das bases de dados, conforme previsto no §2° do art. 18 e no art. 20.

Parágrafo único. Caberá às secretarias de saúde dos Estados, Municípios, Distrito Federal e entidades vinculadas ao Ministério da Saúde identificar as instâncias competentes para a análise

recursal, observados os ditames desta Resolução e da Lei nº 12.527, de 18 de novembro de 2011.

CAPÍTULO IX DA GERAÇÃO DA CÓPIA E ENTREGA

Art. 27. Havendo autorização para cessão de base de dados, o Custodiante providenciará, ante o recebimento do termo de responsabilidade e confidencialidade referido no art. 17, uma cópia da base a ser cedida, com os devidos procedimentos de segurança, o dicionário de dados e o histórico de alterações de estrutura de objetos, quando disponíveis, que serão gravados em mídia segura ou enviados por meios de transferência em canais seguros de comunicação.

§ 1º A entrega da mídia referida no "caput" deverá ser feita presencialmente pelo Custodiante, ou agente público por ele autorizado, ao solicitante ou a pessoa relacionada no termo de responsabilidade e confidencialidade referido no art. 17.

§ 2º A cópia da base de dados contendo dados pessoais será encriptada, por padrão de criptografia recomendado pelo Custodiante, e a chave de decriptação será passada com segurança e confidencialidade para o solicitante, em separado.

CAPÍTULO X DAS RESPONSABILIDADES

Seção I – Solicitante

Art. 28. Conforme o termo de responsabilidade e confidencialidade, previsto no art. 18, o solicitante comprometer-se-á a:

I - guardar sigilo e zelar pela privacidade das pessoas e fatos relacionados ou listados nas informações da base de dados acessada ou cedida;

II - não realizar contatos ou visitas ao domicílio da família da pessoa, cuja informação pessoal fora disponibilizada, para quaisquer tipos de complementação de informação, devendo usar os registros dos sistemas de informação apenas como fonte de informação do endereço e outros dados sobre o evento em saúde;

III - guardar sigilo sobre eventuais senhas fornecidas para acesso à base de dados contendo informações pessoais em saúde;

IV - não repassar, comercializar ou transferir a terceiros as informações individualizadas obtidas da base de dados acessada ou cedida;

V - não disponibilizar, emprestar ou permitir acesso de pessoas ou instituições não autorizadas às informações pessoais em saúde disponibilizadas;

VI - guardar os dados contendo informações pessoais cedidas e manipuladas em mídias e locais que não permitam o acesso, físico ou lógico, de pessoas não autorizadas;

VII - não divulgar, por qualquer meio, inclusive nos relatórios de conclusão de pesquisa, dados ou informações contendo os nomes ou quaisquer outras variáveis que permitam a identificação de indivíduos ou que afetem a confidencialidade das informações pessoais em saúde;

VIII - não praticar ou permitir qualquer ação que comprometa a integridade da base de dados originalmente cedida;

IX - utilizar as informações contidas nas bases de dados exclusivamente para as finalidades descritas no formulário de solicitação e aprovadas pelo Gestor da Informação do sistema de informação correspondente;

X não utilizar isoladamente as informações contidas nas bases de dados acessadas ou cedidas para tomar decisões sobre a identidade das pessoas relacionadas nas bases, para fins de benefício ou outros tipos de atos restritivos de direitos ou punitivos, sem a devida certificação dessas identidades a partir de outras fontes;

XI - não gerar cópias dos dados recebidos, para outras mídias, ou discos rígidos, mas, caso precise fazê-lo, apagar de modo a não permitir a recuperação total ou parcial das informações, ao final da apuração dos resultados;

XII - inutilizar a mídia em que recebeu os dados gravados de modo a não permitir a recuperação total ou parcial das informações, após a sua utilização;

XIII - reportar ao Gestor da Informação limitações encontradas durante a utilização dos dados acessados ou cedidos, resultantes de problemas com a qualidade ou integridade desses dados; e

XIV - comunicar imediatamente o Gestor da Informação caso haja quebra de segurança da informação.

Art. 29. Para os casos previstos no inciso II do art. 5°, o solicitante, além de atender aos incisos do art. 28, deve:

I - mencionar no estudo o Concedente como fonte de informação, o período de referência dos dados cedidos e explicitar que as interpretações decorrentes das informações analisadas são do próprio autor;

II - encaminhar ao Gestor da Informação, semestralmente, relatório informando o andamento do estudo e cópia do relatório final, quando se tratar de pesquisa acadêmica ou científica; e

III - encaminhar ao Gestor da Informação, após a publicação do resultado final do estudo, cópia da base de dados gerada como produto de operações de relacionamento de dados e documentação, informando o método utilizado.

Art. 30. Quando o dispositivo de mídia eletrônica que contenha a base de dados cedida não puder ser inutilizado, nos termos do inciso XII do art. 28 o solicitante deverá descartar os dados de forma a não permitir a recuperação total ou parcial das informações.

Art. 31. O não cumprimento das medidas e condições constantes do termo de responsabilidade e confidencialidade, de que trata o art. 17 sujeitará o solicitante às penalidades legais aplicáveis.

Seção II – Agente Público Autorizado

Art. 32. Agentes Públicos Legalmente Autorizados que tiverem acesso às bases de dados confidenciais custodiadas pelo Sistema Único de Saúde devem guardar sigilo quanto ao seu conteúdo e:

I - não repassar ou transferir o conteúdo de bases de dados a terceiros durante a vigência e após o término do contrato de trabalho ou de prestação de serviço; e

II - não divulgar ou se apropriar de informações contidas nas bases de dados contendo informações pessoais que tenham sido usadas, criadas ou mantidas sob seu controle.

Seção III – Custodiante e Gestor da Informação

Art. 33. Compete ao Custodiante:

I - adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de

acessos e cessões não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer outra forma de tratamento inadequado ou ilícito; e

II - implementar técnicas avançadas de desidentificação e de processos para vinculação de dados pessoais que envolvam as bases de dados distintas sob sua custódia, com o objetivo principal de evitar a cessão de dados pessoais que tenham como argumento em suas solicitações a necessidade de relacionar bancos de dados.

Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia do Custodiante, com a natureza dos dados e com as características específicas do tratamento, considerando-se os Princípios Gerais de Proteção de Dados Pessoais em Saúde, previstos nesta Resolução, e a Política de Segurança da Informação e Comunicações do Ministério da Saúde (POSIC/MS).

Art. 34. O Gestor de Custódia deve indicar os agentes públicos legalmente autorizados responsáveis pelo acesso e tratamento dos dados referentes às informações pessoais em saúde e manter atualizadas as informações para contato com estes agentes.

§1° O agente público legalmente autorizado ou qualquer outro que intervenha em uma das fases do tratamento dos dados obriga-se, mediante termo de responsabilidade devidamente assinado e renovado a cada 6 (seis) meses, ao dever de sigilo em relação às informações pessoais em saúde; e

§2° O agente público legalmente autorizado deve manter registro das operações realizadas para efeito de tratamento de dados pessoais em saúde, e enviar, periodicamente, relatório atualizado ao Gestor de Custódia.

Art. 35. Compete ao Gestor da Informação zelar pelas informações pessoais presentes no sistema de informação sob sua responsabilidade e ainda alertar ao respectivo Custodiante sobre a necessidade de proteção do banco de dados correspondente.

CAPÍTULO XI – DAS PENALIDADES

Art. 36. Constituem condutas ilícitas que ensejam responsabilidades aos agentes públicos aquelas dispostas no art. 32 da Lei 12.527 de 2012.

Art. 37. A pessoa física ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o poder público e deixar de observar o disposto nesta Resolução estará sujeita às sanções previstas no art. 33 da Lei 12.527 de 2012.

Art. 38. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da cessão, acesso ou divulgação não autorizada ou utilização indevida de informações pessoais em saúde, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso, conforme art. 33 da Lei 12.527 de 2012.

Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação pessoal em saúde e a submeta a tratamento indevido, conforme parágrafo único do art. 33 da Lei 12.527 de 2012.

Art. 39. Aquele que obtiver, sem anuência, acesso às informações pessoais de terceiros, será responsabilizado por seu uso e no caso de utilização indevida, estará sujeito a penalidades na forma da lei.

CAPÍTULO XII – DISPOSIÇÕES FINAIS

Art. 40. Caberá às secretarias estaduais e municipais de saúde, bem como às entidades vinculadas ao Ministério da Saúde, caso julguem necessário, a elaboração de procedimentos e normas complementares relativos ao acesso ou cessão de informações pessoais em saúde, em conformidade com esta Resolução.

Art. 41. As áreas gestoras cujas bases de dados não se encontram sob a custódia do Datasus, no âmbito do Ministério da Saúde, deverão se adequar ao trâmite disposto nesta Resolução, de acordo com sua estrutura organizacional.

Art. 42. Os casos de acesso ou cessão de bases de dados contendo informações pessoais custodiadas pelo SUS não tratados nesta Resolução deverão ser apreciados pelo CIINFO, ou pelo Comitê Gestor da Estratégia e-Saúde, quando extrapolarem o âmbito das competências do Ministério da Saúde.

Art. 43. Esta Resolução entra em vigor na data de sua publicação.

RICARDO JOSÉ MAGALHÃES BARROS
MICHELE CAPUTO NETO

MAURO MAGALHÃES JUNQUEIRA