POLÍTICA

EBSERH/SEDE

Política de Proteção de Dados Pessoais da Rede Ebserh

Versão: 2 | 2024

SUS

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

PRESIDENTE

ADEMAR ARTHUR CHIORO DOS REIS

VICE- PRESIDENTE

DANIEL GOMES MONTEIRO BELTRAMMI

ELABORAÇÃO

Diego Henrique de Souza Rezende - Ouvidoria

Pollyana da Silva Alcântara - Conjur

José Santos Souza Santana – ACCIGR

VALIDAÇÃO

José Santos Souza Santana - ACCIGR

APROVAÇÃO

Ademar Arthur Chioro dos Reis – Presidente

Data da Emissão: xx/xx/2024

Código do documento: POL.ACCIGR.002

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA REDE EBSERH

Dispõe sobre definições, princípios, diretrizes, deveres e direitos a serem observados para a proteção de dados pessoais no âmbito da Empresa Brasileira de Serviços Hospitalares (Ebserh).

CAPÍTULO I

DO OBJETO E ÂMBITO DE APLICAÇÃO

Art. 1º O objetivo desta Política é dispor sobre definições, princípios, diretrizes, deveres e direitos a serem observados para a proteção de dados pessoais no âmbito da Empresa Brasileira de Serviços Hospitalares (Ebserh) em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo único. A presente Política se aplica àqueles que integram a Ebserh, assim como a outras pessoas físicas ou jurídicas que, de alguma forma, se relacionem com a empresa.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 2º Para os fins desta Política, considera-se:

I - Administração Central: constituída pelos Órgãos Sociais e Estatutários, pela Presidência, Vice-Presidência e Diretorias da Ebserh, juntamente com as suas áreas vinculadas, cuja competência prioritária é a gestão da Rede Ebserh;

II - agentes de tratamento: o controlador e o operador;

III - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

IV - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional;

V - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

VI - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

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

VIII - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IX - dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

X - dado pessoal sensível: informação sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XI - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XIII - filiais: Hospitais Universitários Federais (HUFs) geridos pela Ebserh, por meio de contrato de gestão especial firmado com as Universidades Federais, para a prestação de serviços de ensino, pesquisa e de atenção à saúde;

XIV - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XV - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVI - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XVII - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVIII - tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; e

XIX - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 3º A proteção de dados pessoais é valor primordial e o tratamento de dados pessoais deve ser cautelosamente avaliado e realizado com observância das diretrizes dispostas nesta Política e na legislação aplicável.

Art. 4º Todo tratamento de dados pessoais realizado no âmbito da Rede Ebserh deve contar com finalidade legítima e específica e estar amparado em uma das disposições previstas na Lei Geral de Proteção de Dados Pessoais.

Art. 5º O tratamento de dados pessoais realizado no âmbito da Rede Ebserh deve observar a boa-fé e os seguintes princípios:

I - finalidade: deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: deve ser garantido ao titular dos dados pessoais a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: devem ser garantidas ao titular dos dados pessoais a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: devem ser garantidas ao titular dos dados pessoais informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos inerentes à atividade;

VII - segurança: devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 6º A Administração Central e as filiais devem proteger, mapear e registrar o tratamento de dados pessoais realizados no âmbito de suas atuações.

Art. 7ª Os contratos que envolvam tratamento de dados pessoais em nome do controlador devem conter cláusulas que estabeleçam instruções, deveres e obrigações referentes ao tema e o compromisso dos contratados em adotar medidas para adequação de suas operações e cumprimento das legislações de proteção de dados pessoais aplicáveis, bem como desta Política e demais normas e orientações da Ebserh.

Art. 8º A Ebserh deve implementar meios para conferir a transparência necessária aos titulares em

relação ao uso de seus dados pessoais, à finalidade, forma e duração do tratamento, identificação e informações de contato do controlador e do encarregado, informações acerca do uso compartilhado de dados, responsabilidades dos agentes envolvidos e demais direitos dos titulares de dados pessoais.

Art. 9º A Administração Central e as filiais devem implementar mecanismos efetivos para atendimento dos direitos dos titulares previstos em lei, como informação, acesso, retificação, portabilidade, eliminação, bloqueio, revogação de consentimento, dentre outros.

Art. 10. O relatório de impacto à proteção de dados pessoais deve ser elaborado sempre que o tratamento de dados pessoais for capaz de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais ou quando solicitado pela Autoridade Nacional de Proteção de Dados.

Art. 11. A Administração Central e as filiais devem divulgar e manter atualizadas, em seu sítio eletrônico, a identidade e as informações de contato do encarregado pelo tratamento de dados pessoais.

Art. 12. A Ebserh tratará os dados pessoais em seus próprios sistemas e programas, inclusive por intermédio de terceiros legalmente constituídos, para tanto:

I - utiliza métodos para criptografar e anonimizar os dados coletados;

II - possui proteção contra acesso não autorizado a seus sistemas;

III - autoriza o acesso de pessoas previamente estabelecidas ao local onde são armazenadas as informações coletadas;

IV - cobra de terceiros a manutenção de sigilo, sendo que a quebra acarretará responsabilidade civil e responsabilização conforme a legislação; e

V - envida esforços para preservar a privacidade dos dados dos usuários e estimula estes à autoproteção de seus dados pessoais.

Art. 13. A Administração Central e as filiais devem criar planos de resposta a incidentes que envolvam dados pessoais observado o disposto no Plano de Gestão de Incidentes Cibernéticos da Ebserh.

Art. 14. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos inerentes à atividade;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Art. 15. Ao tomar conhecimento de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, caberá à Administração Central, juntamente com a filial respectiva, analisar a ocorrência e pontuar a gravidade e se houve atendimento das diretrizes desta Política, em especial no que diz respeito aos planos de resposta a incidentes que envolvam dados pessoais.

§1º Após a adoção das medidas mencionadas no caput deste artigo, a Administração Central e filiais envolvidas no incidente de segurança deverão fornecer ao controlador os devidos subsídios para que esse efetive a comunicação à autoridade nacional e ao titular.

§2º As filiais, quando da apresentação de subsídios ao controlador, deverão fazê-la em alinhamento com a Administração Central.

Art. 16. A Administração Central deve ser sempre comunicada nos casos de incidentes de segurança que envolvam dados pessoais, sejam eles sensíveis ou não.

Art. 17. Toda operação que envolva transferência internacional de dados pessoais deve possuir salvaguardas, previstas na Lei Geral de Proteção de Dados Pessoais, considerando o nível de proteção de dados do país estrangeiro ou do organismo internacional do qual o país seja membro.

Art. 18. A Rede Ebserh deve promover a conscientização dos colaboradores acerca das diretrizes e procedimentos de proteção de dados pessoais implementados.

CAPÍTULO V

DO TRATAMENTO DE DADOS PESSOAIS

Art. 19. O tratamento de dados pessoais no âmbito da Ebserh será realizado para o atendimento de sua finalidade pública, conforme o interesse público, com o objetivo de executar competências legais e de cumprir as atribuições legais do serviço público.

Parágrafo único. Os dados pessoais deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado nos termos da LGPD, de forma a facilitar seu uso quando necessário.

Art. 20. Toda e qualquer atividade de tratamento de dados pessoais será registrada, desde a sua coleta até o seu descarte, indicando quais tipos de dados pessoais serão coletados, a base legal que autoriza os seus usos, as suas finalidades, o tempo de retenção, as práticas de segurança de informação implementadas no armazenamento, e com quem os dados podem ser eventualmente

compartilhados, segundo o inventário de dados.

Art. 21. O tratamento de dados pessoais somente será realizado mediante o fornecimento de consentimento pelo titular dos dados, salvo nos casos excepcionados pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 22. O tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas, salvo quanto às exceções previstas na Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 23. O tratamento de dados pessoais e dados pessoais sensíveis de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas na Lei Geral de Proteção de Dados Pessoais, desde que observado o seu melhor interesse, a ser avaliado no caso concreto, observados os termos da legislação pertinente.

Art. 24. Quando a base legal do tratamento for o consentimento, a Rede Ebserh deve implementar mecanismos adequados para a efetiva coleta da autorização nos termos da lei e, assim, evidenciar a regularidade do tratamento.

Art. 25. Caso o consentimento indispensável não seja concedido, o tratamento de dados pessoais e dados pessoais sensíveis não será realizado.

Art. 26. O compartilhamento de dados pessoais ocorrerá somente em situações de justificada necessidade, com finalidade e tratamento claramente especificados, bem como com a aplicação das medidas necessárias para registro, controle, proteção, sincronização, eliminação, anonimização e bloqueio dos dados pessoais compartilhados.

Art. 27. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto na LGPD.

Art. 28. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Art. 29. No âmbito da Ebserh são considerados como titulares de dados pessoais:

I - pacientes, seus responsáveis legais e acompanhantes;

II - empregados, servidores que se encontrem desempenhando suas atividades na Rede Ebserh e ocupantes de cargos de confiança, e seus dependentes;

III - estudantes, estagiários, residentes, professores e pesquisadores;

IV - profissionais de empresas terceirizadas, colaboradores em geral e todos aqueles que, de forma individual ou coletiva, por força de lei, contrato ou qualquer outro ato jurídico, se relacionam ou atuem na prestação de serviços à Rede Ebserh, de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, direta ou indiretamente; e

V - outras pessoas que tiverem seus dados pessoais sob os cuidados, ainda que temporariamente, da Rede Ebserh, seja no âmbito da Administração Central ou das filiais.

CAPÍTULO VI

DO CONTROLADOR, ENCARREGADO E OPERADORES

Seção I - Do Controlador

Art. 30. A Ebserh, enquanto pessoa jurídica de direito privado, exerce o papel de controladora dos dados pessoais coletados no âmbito da empresa.

Art. 31. São atribuições do controlador:

I - supervisionar o cumprimento desta Política, estabelecendo medidas para garantir a proteção de dados pessoais;

II - observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre tratamento ou de realizá-lo;

III - elaborar o relatório de impacto à proteção de dados pessoais;

IV - informar previamente o titular sobre as mudanças de finalidade para o tratamento de dados pessoais;

V - adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse;

VI - fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos inerentes à atividade;

VII - indicar o encarregado pelo tratamento de dados pessoais no âmbito da Ebserh;

VIII - comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

IX - manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse; e

X - exercer outras funções impostas pela legislação vigente.

Seção II - Do Encarregado

Art. 32. A função de encarregado será exercida pelo(a) Ouvidor(a)-Geral da Ebserh.

Art. 33. São atribuições do encarregado:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os colaboradores e aqueles que, de alguma forma, se relacionem com a Ebserh, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); e

V - executar as demais atribuições determinadas pelo controlador ou estabelecidas pela legislação.

Seção III - Dos Operadores

Art. 34. São considerados como operadores todos aqueles que realizam o tratamento de dados pessoais coletados no âmbito da Ebserh.

Art. 35. São atribuições dos operadores:

I - observar os princípios estabelecidos nesta Política, ao realizar tratamento de dados pessoais;

II - realizar o tratamento de dados pessoais segundo as instruções fornecidas pelo controlador;

III - manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse; e

IV - exercer outras funções impostas pela legislação vigente.

CAPÍTULO VII

DAS MEDIDAS DE SEGURANÇA E BOAS PRÁTICAS

Art. 36. No âmbito da Ebserh devem ser adotadas medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou de qualquer forma de tratamento inadequado ou ilícito.

Art. 37. Para proteger os dados pessoais do titular, a Ebserh adotará medidas adequadas aos casos e com base em critérios de riscos, tais como:

I - Criptografia;

II - Anonimização e pseudonimização;

III - Proteção contra acesso não autorizado a sistemas;

IV - Proteção contra acesso físico e lógico;

V - Auditoria;

VI - Monitoramento e detecção;

VII - Compromisso de manutenção do sigilo;

VIII - Manutenção do inventário de dados pessoais;

IX - Limitação do acesso aos dados pessoais conforme a finalidade da atividade a ser desenvolvida;

X - Plano de resposta a incidentes relacionados à proteção de dados pessoais;

XI - Aplicação de sanções decorrentes de incidentes;

XII - Elaboração de termos de confidencialidade, termos de responsabilidade ou termos de sigilo a serem assinados pelos operadores;

XIII - Proteção de dados desde a concepção e por padrão;

XIV - Capacitação dos colaboradores que tratam dados para atualização permanente sobre medidas de proteção; e

XV - Outras medidas consideradas como necessárias para a proteção dos dados pessoais nos termos da legislação.

Art. 38. Os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Art. 39. A anonimização de dados pessoais deve ser realizada com o propósito de mitigar os riscos de violação de dados.

Art. 40. Antes de realizar a anonimização de dados pessoais, será verificado se, no ciclo devido de tratamento dos dados, foram observados os princípios da finalidade, adequação, necessidade e qualidade dos dados.

CAPÍTULO VIII

DOS DEVERES DOS RESPONSÁVEIS PELO TRATAMENTO DE DADOS PESSOAIS

Art. 41. Os responsáveis pelo tratamento de dados pessoais no âmbito da Rede Ebserh devem observar, dentre outros previstos na legislação, os seguintes deveres:

I - não disponibilizar, nem garantir acesso aos dados pessoais mantidos pela Ebserh para pessoas não autorizadas ou competentes de acordo com as normas da empresa e legislação vigente;

II - obter o consentimento do titular ou do responsável, quando necessário e conforme o caso, para o tratamento de dados pessoais;

III - cumprir as normas, recomendações, orientações de segurança da informação e prevenção de incidentes de segurança da informação publicadas pela Ebserh; e

IV - comunicar ao Encarregado pelo Tratamento de Dados Pessoais qualquer evento que possa colocar em risco os dados pessoais tratados pela Rede Ebserh.

CAPÍTULO IX

DOS DIREITOS DO TITULAR DE DADOS PESSOAIS

Art. 42. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - Finalidade específica do tratamento;

II - Forma e duração do tratamento, observados os segredos inerentes à atividade;

III - Identificação do controlador;

IV - Informações de contato do controlador;

V - Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - Responsabilidades dos agentes que realizarão o tratamento; e

VII - Direitos do titular, com menção explícita aos direitos expostos nesta Política.

Art. 43. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - A confirmação da existência de tratamento;

II - O acesso aos dados;

III - A correção de dados incompletos, inexatos ou desatualizados;

IV - A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - A eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 28 desta Política;

VI - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

VIII - A revogação do consentimento.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 44. A Administração Central deve editar recomendações gerais para o tratamento de dados pessoais, respeitadas as disposições da presente Política.

Art. 45. A Administração Central e as filiais devem dar ciência desta Política de Proteção de Dados Pessoais aos fornecedores, prestadores de serviços e demais partes que, de alguma forma, se relacionem com a Ebserh.

Art. 46. O cumprimento desta Política, bem como dos normativos que a complementam, devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 47. Os agentes envolvidos em eventual transgressão às diretrizes dispostas nesta Política estarão sujeitos à responsabilização, nos termos dos normativos internos e legislação aplicável.

Art. 48. Esta Política poderá ser modificada no todo ou em parte em caso de necessidade de atualização dos seus termos, conforme legislação em vigor.

Parágrafo único. A proposta de alteração deverá ser submetida à deliberação do Conselho de Administração da Ebserh, com prévia manifestação da Diretoria Executiva.

Art. 49. Esta Política entra em vigor na data da sua publicação em Boletim de Serviço.