Ministério da Saúde
Secretaria de Atenção Primária à Saúde
Departamento de Apoio à Gestão da Atenção Primária

NOTA TÉCNICA Nº 52/2024-DGAPS/SAPS/MS

1. ASSUNTO

1.1. Esclarecimento sobre os procedimentos para solicitação ao acesso a base dados, identificados, pseudononimizados ou anonimizadas não públicas à Cordenação Setorial de Planejamento, Avaliação e dimensionamento de Profissionais da APS - CPLAD**,** com Base nas Leis nº 12.527/2011 e nº 13.709/2018.

2. CONTEXTUALIZAÇÃO

2.1. Os bancos de dados utilizados na gestão dos Programas de Provimento Federal armazenam uma ampla variedade de dados, incluindo informações pessoais sensíveis, como data de nascimento e CPF.

2.2. Existe uma grande demanda de diversos atores (gabinete SAPS, Secretaria Executiva do MS, outras secretarias, sociedade civil por meio de LAI) pelos dados referentes aos Programas de Provimento Federal, principalmente no que tange à quantidade de profissionais em atividade e a flutuação deste quantitativo em série histórica.

2.3. Para maior eficiência no armazenamento, tratamento, consulta, disponibilização e gestão de dados referentes aos Programas de Provimento Federal, os bancos de dados são gerenciados pela SGBD (Sistema de Gerenciamento de Banco de Dados) *PostgreSQL*.

2.4. O dever de implementar medidas de segurança para proteger os dados pessoais está em conformidade com o Artigo 46 da Lei 13.709/2018, relacionado aos bancos de dados sob gestão

2.5. **Objetivos**

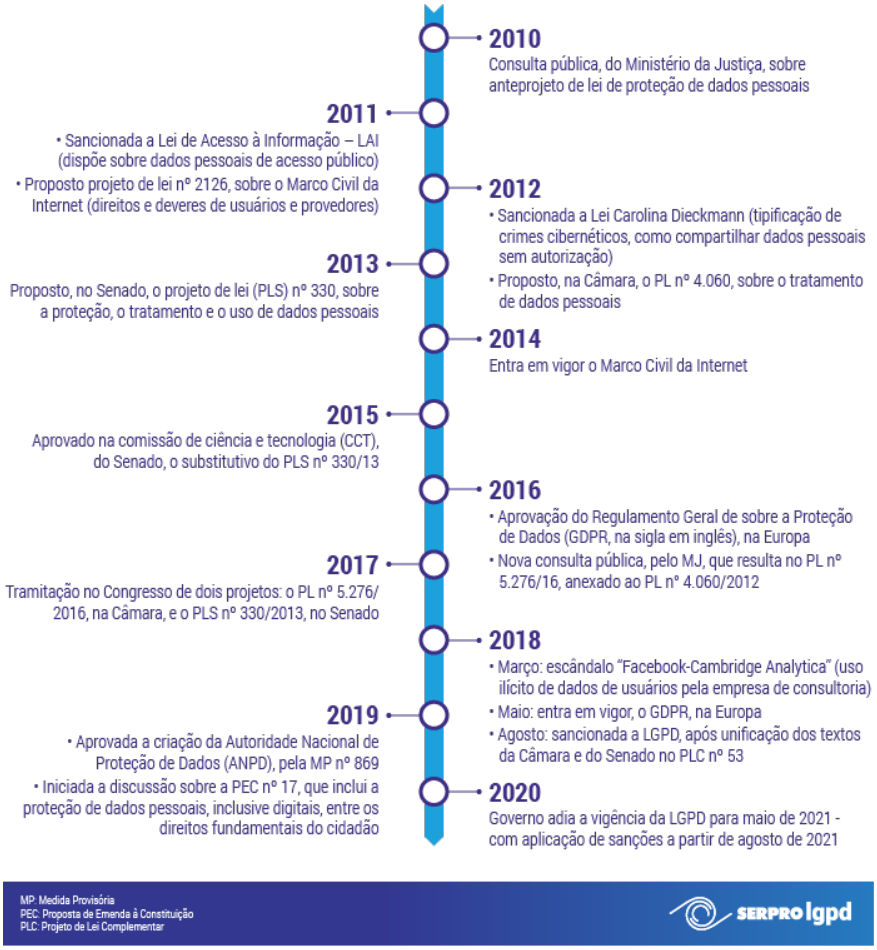
2.5.1. A presente nota técnica visa esclarecer e estabelecer diretrizes claras sobre o processo de solicitação de dados à CPLAD, fundamentado nas Leis nº 12.527/2011 (Lei de Acesso à Informação) e nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD). Buscando promover a transparência, a segurança da informação e o cumprimento rigoroso das normativas legais, contribuindo para a eficiência no armazenamento, tratamento e disponibilização de dados referentes aos Programas de Provimento Federal.

2.5.2. Considerando a ampla demanda por dados provenientes dos Programas de Provimento Federal, nossos objetivos incluem a promoção de práticas que garantam a integridade, confidencialidade e tratamento responsável das informações armazenadas. Buscamos otimizar a gestão e assegurar que o acesso aos dados seja realizado de forma transparente, legalmente respaldada e em conformidade com as leis de proteção de dados.

3. BASE LEGAL

3.1. A Constituição Federal de 1988 assegura o direito dos cidadãos à informação pública. Inicialmente, houve interpretação restritiva, mas ao longo do tempo, foram estabelecidos leis, decretos e portarias sobre o acesso às informações públicas.

3.2. A Figura 1 apresenta a linha do tempo relacionada à proteção de dados.



Fonte: SERPRO https://www.serpro.gov.br/lgpd/noticias/2020/protecao-de-dados-avanca-pais - 15/05/2024

3.3. A Lei de Acesso à Informação (LAI) - Lei nº 12.527, de 18 de novembro de 2011, regulamentou o direito constitucional à informação. Seu propósito foi assegurar que todos tenham acesso a informações de interesse particular, geral ou coletivo, fornecidas pelos órgãos públicos. Além disso, a Lei Geral de Proteção de Dados (LGPD), sancionada em 14 de agosto de 2018, aborda diretamente essa questão, estabelecendo diversos direitos e garantias para os titulares dos dados, bem como obrigações e responsabilidades para os controladores das informações.

3.4. O Decreto Nº 10.046, de 09 de outubro de 2019, introduz novas definições para tipos de dados e estabelece a necessidade de os gestores da informação categorizarem o nível de compartilhamento dos dados. Especificamente em relação aos dados de saúde, a categorização do compartilhamento como “específico” indica que o conjunto de bases de dados possui restrições de acesso. As razões para tais restrições devem ser claramente delineadas, e a classificação deve ser revisada a cada cinco anos, ou sempre que houver mudanças nas diretrizes que levaram à sua categorização.

3.5. A Portaria Nº 884, de 13 dezembro de 2011, do Ministério da Saúde, estabelece as diretrizes e procedimentos para a solicitação e cessão de dados dos bancos nacionais dos Sistemas de Informação gerenciados pela Secretaria de Atenção à Saúde. Define as responsabilidades dos solicitantes em relação ao uso adequado, sigilo e privacidade dos dados, bem como os passos a serem seguidos para a análise e liberação das informações solicitadas. Visa garantir a segurança e a confidencialidade dos dados, bem como o uso ético e legal das informações disponibilizadas.

4. DEFINIÇÕES

4.1. Para fins deste documento, o **Quadro 1** apresenta os principais termos e definições com base na Portaria GSI/PR nº 93 de 26 de setembro de 2019.

Quadro 1. Principais termos e definições utilizados pelo protocolo de acesso a dados identificados

Termo	Definição
Agente público	Todo aquele que exerce, 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 dados com informações pessoais em saúde. (Lei nº 8.429/1992)
Agente público legalmente autorizado	Todo servidor da administração pública, concursado ou comissionado, que possui condição pessoal (competências legais próprias da carreira) – 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
Agentes de tratamento	O controlador e o operador (Lei nº 13.709/2018, LGPD, art. 5º).
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. (Lei nº 13.709/2018, LGPD, art. 5º, XI)
Base de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (Lei nº 13.709/2018, LGPD, art. 5º, IV)
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Lei nº 13.709/2018, LGPD, art. 5º, VI)
Criptografia	Cifração, com o emprego de algoritmos matemáticos e parâmetros de controle chamados de chaves criptográficas, busca tornar a mensagem incompreensível e inútil para todos os efeitos, enquanto não for submetida ao processo inverso de decifração. (Guia de Interoperabilidade – Governo digital)
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável (Lei nº 13.709/2018, LGPD, art. 5º, I)
Dado sensível	Dado pessoal 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. (Lei nº 13.709/2018, LGPD, art. 5º, II)
Dados Cadastrais	Informações identificadoras perante os cadastros de órgãos públicos (art. 2º inciso III Decreto nº 10.046/2019). Inclui entre números nacionais de identificação número de inscrição no Programa, o número do registro no CRM e ou RMS, o número do CNS, pois são dados identificatórios e se relacionam a uma pessoa específica.
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). (Lei nº 13.709/2018, LGPD, art. 5º, VIII

Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (Lei nº 13.709/2018, LGPD, art. 5º, VII)
Pseudonimizado	Possibilidade de reversão do processo que obteve a anonimização, permitindo a reidentificação do titular de dados. (Guia De Boas Práticas - Lei Geral De Proteção De Dados (LGPD))
Segurança da informação	Capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação.
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. (Lei nº 13.709/2018, LGPD, art. 5º, V)
Tratamento	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (Lei nº 13.709/2018, LGPD, art. 5º, X)
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. (Lei nº 13.709/2018, LGPD, art. 5º, XVI)

Acesso a base de dados

4.2. **Documentação**

4.2.1. Etapa comum aos diferentes solicitantes, conferência da documentação, conforme apresentado no **Quadro 2**

Quadro 2. Documentos necessários para solicitação de dados

Solicitante	Documentos
Titular	Requerimento ou declaração com a solicitação da informação de forma clara, no caso de dados sob gestão da CPLAD, deverá conter informações, como, nome completo do titular, data de nascimento, além de anexada cópia de documento de identidade, que deverá ser verificado e validado por agente público.
Unidades do Ministério da Saúde	Ofício institucional (via SEI) contendo informações sobre o pedido, assim como a finalidade baseada na execução de políticas públicas, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador; além do preenchimento e assinatura Termo de Responsabilidade e Confiabilidade (anexo I) (0040757706).
Órgãos da Administração Pública Federal	Ofício institucional (via SEI) contendo informações sobre o pedido, assim como a finalidade baseada na execução de políticas públicas, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador; justificativa para ter acesso a dados pessoais sensíveis de saúde (quando fora de sua competência) e justificativa de ter acesso a dados fora da sua área de abrangência; além de preenchimento e assinatura Termo de Responsabilidade e Confiabilidade (anexo I) (0040757706) .
Órgãos de Justiça / Ministério Público	Ofício institucional (via SEI) contendo informações sobre o pedido, assim como a finalidade baseada na execução de inquérito civil, além de preenchimento e assinatura Termo de Responsabilidade e Confiabilidade (anexo I).

Pesquisadores	Ofício da instituição encaminhando a documentação abaixo: • Protocolo/Projeto de pesquisa; • Termo de responsabilidade assinado (Portaria nº 884/2011 e Artigo 61 do Decreto nº 7.724/2012) (0040819980); • Currículo Lattes atualizado do(a) pesquisador(a) titular e dos eventuais pesquisadores(as) auxiliares; • Documento que comprove que o(a) solicitante é pesquisador(a) vinculado(a) a Instituição declarada no Termo de Responsabilidade; • Documento de aprovação no Comitê Nacional de Ética em Pesquisa; • Fotocópia do documento de identidade ou do Conselho de Classe; e • Fotocópia do CPF.

5. ACESSO INTERNO ÀS BASES DE DADOS PELAS UNIDADES DO MINISTÉRIO DA SAÚDE

5.1. Os bancos de dados sob responsabilidade da Coordenação Setorial de Planejamento, Avaliação e Dimensionamento da APS (CPLAD) são disponibilizados na rede corporativa interna do Ministério da Saúde, gerida pelo Departamento de Informática do SUS - DataSUS.

5.2. É importante ressaltar que, devido à presença de dados pessoais sensíveis, essas bases não devem ser consideradas anonimizadas. O acesso está vinculado ao login "@saude.gov.br" do agente público, para uso interno, visando cumprir rotinas das áreas técnicas. Não é permitida a transmissão de dados nominais por e-mail ou outras formas não seguras, nem a disponibilização por meio de diretórios compartilhados em rede (local ou virtual) ou mídias externas (*pendrive*, CD, DVD, etc.). O armazenamento local das bases de dados pelo agente público deve ser feito em pasta protegida, de acesso restrito, conforme as sanções administrativas previstas no art. 52 da Lei nº 13.709/2018.

5.3. O acesso a essas bases de dados deve seguir o mesmo fluxo de solicitação de acesso aos outros sistemas sob responsabilidade do DataSUS, por meio de preenchimento do **Termo de Responsabilidade**. Nele deve ser especificado qual(is) esquema(s) deseja ter acesso, o detalhamento das necessidades de acesso, a finalidade do acesso e o período de validade. Após preenchimento desta etapa deve-se preencher os campos de identificação do solicitante, o de identificação do responsável pelo manuseio/acesso e o de identificação do gestor do banco do sistema fornecedor.

5.4. Preenchendo o termo deve-se abrir um processo via SEI e gerar um ofício com as informações solicitadas no termo e despachar para a coordenação responsável pelo banco de dados, neste caso à CPLAD. Que tomará as devidas providências para o acesso ao banco de dados.

6. SOLICITAÇÃO DE ACESSO AO BANCO DE DADOS IDENTIFICADOS POR OUTROS ÓRGÃOS

6.1. O compartilhamento de dados entre instituições, de acordo com as leis nº 13.709/2018 e Decreto nº 10.046/2019, estabeleceu novas regras no âmbito da Administração Pública Federal. O acesso a dados pessoais deve ser vinculado à persecução do interesse público, com a indicação de um encarregado para o tratamento dos dados.

6.2. Agentes públicos legalmente autorizados, como servidores da área de saúde ou gestão, podem acessar os bancos de dados para realizar suas atividades. Servidores de outros órgãos que necessitam de dados dos sistemas custodiados pelo Ministério da Saúde para qualificação de seus dados e/ou melhoria de serviços e benefícios aos titulares dos dados também são considerados.

6.3. Conforme a Portaria nº 884/2011 e o Decreto nº 7.724/2012, o acesso à informação pessoal por terceiros requer a assinatura de um termo de responsabilidade, detalhando a finalidade e destinação da autorização, bem como as obrigações do requerente, vinculadas à finalidade autorizada, sob pena de uso indevido.

6.4. Ao solicitar dados restritos das bases, os órgãos e entidades devem declarar o comprometimento em cumprir os requisitos de segurança exigidos para o nível de compartilhamento restrito e específico, conforme o Art. 12, § 1º do Decreto nº 10.046/2019.

7. PESQUISADORES(AS)

7.1. Para projetos de pesquisa de graduação ou pós-graduação, os pesquisadores(as) vinculados a uma instituição devem enviar um ofício contendo informações sobre a finalidade e justificativas para a necessidade de acesso aos dados juntamente com os documentos listados abaixo:

a) Protocolo/Projeto de pesquisa;

b) Termo de responsabilidade assinado (Portaria nº 884/2011 e Artigo 61 do Decreto nº 7.724/2012) (0040819980);

c) Currículo Lattes atualizado do(a) pesquisador(a) titular e dos eventuais pesquisadores(as) auxiliares;

d) Documento que comprove que o(a) solicitante é pesquisador(a) vinculado(a) a Instituição declarada no Termo de Responsabilidade;

e) Documento de aprovação no Comitê Nacional de Ética em Pesquisa;

f) Fotocópia do documento de identidade ou do Conselho de Classe; e

g) Fotocópia do CPF.

7.2. Informamos que, após o recebimento da documentação pela CPLAD, será instruído um processo no Sistema Eletrônico de Informações (SEI) do Ministério da Saúde.

7.3. Informamos que o compartilhamento de dados deve ocorrer de forma segura, utilizando a ferramenta de criptografia VeraCrypt, disponibilizada pelo Ministério da Saúde para o compartilhamento seguro de arquivos.

8. CONCLUSÃO

8.1. Em síntese, reconhecemos o potencial dos bancos de dados para ampliar o conhecimento científico e respaldar políticas públicas em saúde. O Ministério da Saúde, ao gerir essas informações, tem dedicado esforços para conciliar esse avanço com a preservação da confidencialidade, a proteção da privacidade individual, o respeito aos termos de consentimento e a gestão eficaz da segurança dos dados. Em consonância com a Lei Geral de Proteção de Dados (LGPD), destacamos a importância de garantir a anonimização adequada, o tratamento responsável dos dados sensíveis e a implementação de medidas de segurança robustas.

8.2. Ademais, ressaltamos que o acesso aos dados deve ser balizado por procedimentos transparentes e legalmente respaldados, conforme delineado nas normativas vigentes. É imperativo que as instituições solicitantes observem rigorosamente as diretrizes estabelecidas, incluindo a designação de encarregados e a adoção de práticas que assegurem a integridade e confidencialidade das informações.

8.3. Nesse contexto, é essencial que todos os envolvidos, sejam eles operadores, controladores ou solicitantes, compreendam e

adiram aos termos desta nota técnica, reconhecendo a responsabilidade que recai sobre cada elo dessa cadeia de tratamento de dados. A transparência, a ética e o compromisso com a segurança da informação são fundamentais para garantir a legitimidade e o sucesso do processo de solicitação de dados, em conformidade não apenas com as leis específicas, mas também com os princípios fundamentais de respeito aos direitos dos titulares de dados.

8.4. Portanto, ao conciliar a busca pelo avanço científico e o cumprimento das normativas legais, a atuação responsável de todos os envolvidos é crucial para assegurar que a utilização desses dados contribua efetivamente para o bem-estar da sociedade, respeitando os mais elevados padrões éticos e legais estabelecidos pela legislação em vigor.

8.5. As atividades propostas incluem:

a) **Protocolos de Acesso:** Estabelecer procedimentos transparentes e legalmente respaldados para solicitação, análise e autorização de acesso aos dados, seguindo os requisitos da LGPD e demais normativas;

b) **Treinamento:** Desenvolver programas de treinamento para os agentes públicos envolvidos, visando a compreensão e adesão aos princípios da LGPD, segurança da informação e ética no tratamento de dados pessoais;

c) **Comunicação Externa:** Elaborar estratégias de comunicação para orientar o público externo sobre como solicitar informações, esclarecendo os procedimentos, requisitos e prazos estabelecidos**,**

d) **Segurança da Informação**: Implementar medidas robustas de segurança da informação, como a criptografia, garantindo a confidencialidade e integridade dos dados, de acordo com as diretrizes da LGPD e da Política Nacional de Segurança da Informação,

e) **Monitoramento e Auditoria**: Estabelecer mecanismos de monitoramento e auditoria contínuos para garantir o cumprimento das normativas, identificar potenciais vulnerabilidades e promover a melhoria contínua dos processos.

8.6. Ao adotar essas ações, busca-se assegurar não apenas a conformidade legal, mas também a contribuição efetiva para o bem-estar da sociedade, respeitando os direitos dos titulares de dados e promovendo a confiança na utilização responsável dessas informações.

8.7. Esta conclusão reforça a necessidade de todos os envolvidos compreenderem e aderirem aos termos desta nota técnica, promovendo a transparência, ética e comprometimento com a segurança da informação em todas as etapas do processo de solicitação de dados

9. REFERÊNCIAS

9.1. Brasil. Lei n° 13.709 de 14 de agosto de 2018. Lei Geral de Proteção dos Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 02 fev. 2024

9.2. Brasil. Decreto n° 10.046 de 09 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em 02 fev. 2024

9.3. Brasil. Lei n° 8.429 de 02 de junho de 1992. 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

https://www.planalto.gov.br/ccivil_03/leis/l8429.htm#:~:text=LEI%20N%C2%BA%208.429%2C%20DE%202%20DE%20JUNHO%20DE%2019 Acesso em 02 fev. 2024

9.4. Decreto nº 9.637 de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a

https://legis.senado.leg.br/norma/30761044#:~:text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,regulamenta%20o%20disposto% . Acesso em 02 fev. 2024

9.5. Decreto nº 7.724 de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm . Acesso em 28 de mar. 2024

9.6. Brasil. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 02 fev. 2024

9.7. Brasil. Guia de Boas Práticas – Lei Geral de proteção de Dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias/guia_lgpd.pdf . Acesso em 02 fev. 2024.

9.8. SERPO. A proteção de dados avança no país. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/protecao-de-dados-avanca-pais. Acesso em 02 fev. 2024

9.9. Portaria nº 884 de 13 de dezembro de 2011 estabelece as diretrizes e procedimentos para a solicitação e cessão de dados dos bancos nacionais dos Sistemas de Informação gerenciados pela Secretaria de Atenção à Saúde. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/sas/2011/prt0884_13_12_2011.html. Acesso em 28 mar. 2024

Documento assinado eletronicamente por **Grasiela Damasceno de Araújo**, **Gerente de Projeto**, em 22/05/2024, às 16:57, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020; e art. 8º, da Portaria nº 900 de 31 de Março de 2017.

Documento assinado eletronicamente por **Wellington Mendes Carvalho**, **Diretor (a) do Departamento de Apoio à Gestão da Atenção Primária**, em 23/05/2024, às 14:40, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020; e art. 8º, da Portaria nº 900 de 31 de Março de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.saude.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0040740342** e o código CRC **BF4D685C**.