Publicações CFF/CRFs em 12/12/2025

CONSELHO FEDERAL DE FARMÁCIA
SHIS - Setor de Habitações Individuais Sul, Lote L, s/n QI 15 - Bairro Lago Sul - CEP 71635-615 - Brasília - DF - www.cff.org.br

PORTARIA Nº 124/2025.

Dispõe sobre a Política de Proteção de Dados Pessoais, no âmbito do Conselho Federal de Farmácia (CFF).

O PRESIDENTE DO CONSELHO FEDERAL DE FARMÁCIA (CFF), no uso de suas competências legais e regimentais, e considerando o direito constitucional da proteção de dados pessoais, previsto no inciso LXXIX do art. 5° da Constituição Federal de 1988;

considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

considerando o disposto no inciso III do art. 6º e no §5º do art. 31 da Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI),

RESOLVE :

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Proteção de Dados Pessoais, no âmbito do Conselho Federal de Farmácia (CFF), obedece ao disposto nesta Portaria.
Parágrafo único. Integra esta Política, como anexo único, a Política de Privacidade e Segurança do Conselho Federal de Farmácia (CFF).

CAPÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS NO CFF

Art. 2º O tratamento de dados pessoais a ser realizado pelo CFF, no desempenho de suas competências e atribuições constitucionais, legais e regulamentares, deve estar em consonância com a finalidade pública.

Art. 3º A realização de tratamento de dados pessoais no âmbito do CFF deve ter como base legal as hipóteses previstas no art. 7º da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

§1º No tratamento a que se refere o caput deste artigo, o CFF utilizará como base legal, preferencialmente, as seguintes hipóteses, independentemente do consentimento dos titulares de dados:

I - cumprimento de obrigação legal ou regulatória, com indicação específica do dispositivo que necessita do tratamento de dados pessoais para ser cumprido; e

II - tratamento e uso compartilhado, pela administração pública, de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições da LGPD acerca do tratamento de dados pessoais pelo poder público.

§ 2º Excetuadas as hipóteses de que trata o parágrafo anterior, a utilização como base legal das demais hipóteses a que se refere o caput deste artigo, dependerá de demonstração motivada com as razões para a sua adoção.

§ 3º No exercício de atividades administrativas não vinculadas diretamente a obrigações legais e ao exercício de suas competências legais e constitucionais, o CFF deverá obter o consentimento dos titulares para tratar dados pessoais, sempre respeitando e concretizando a autodeterminação informativa dos envolvidos.

§ 4º No caso de dados pessoais sensíveis, o tratamento será realizado com base nas disposições previstas pela LGPD.

Art. 4º Quando da utilização do legítimo interesse do CFF para tratamento de dados pessoais, deverão ser:

I – consideradas, além das disposições do art. 10 da LGPD, as situações que envolvam a aproximação com a sociedade, o fomento ao controle social, a preservação histórica, a governança e a gestão sobre seu quadro próprio de pessoal, a manutenção de sua independência e imparcialidade, a defesa de suas competências e atribuições e a segurança institucional (que compreende ativos, informações, patrimônio, autoridades, servidores e colaboradores do Conselho); e

II - observados, além da legislação vigente, os princípios e direitos do titular mencionados nos arts. 6º e 9º da LGPD.

Parágrafo único. A utilização do legítimo interesse como base legal dependerá de motivação expressa da área responsável pelo tratamento de dados pessoais quanto ao equilíbrio entre o interesse do CFF e o do titular dos dados, devendo o Encarregado de Dados do CFF ser consultado.

CAPÍTULO III

DO EXERCÍCIO DOS DIREITOS DO TITULAR

Art. 5º Os direitos do titular de dados pessoais tratados no âmbito do CFF poderão ser exercidos mediante manifestação registrada por meio de correio eletrônico e direcionada ao encarregado de dados, conforme disposto no anexo único desta Política.

Art. 6º Para ter acesso aos sistemas e serviços disponibilizados pelo CFF, inclusive para exercício dos direitos do titular, os usuários deverão, de forma livre e consciente, fornecer dados pessoais necessários ao cadastro, ao credenciamento, à identificação e à autenticação no referido Portal.

Art. 7º Os direitos do titular de dados pessoais previstos na LGPD, em qualquer caso, serão ponderados com o interesse público de conservação de dados históricos, o fomento ao controle social, a preservação da transparência da instituição e das condutas de agentes públicos no exercício de suas atribuições, e com a divulgação de informações relevantes à sociedade.

Art. 8º Nos pedidos de acesso à informação e respectivos recursos, as decisões que tratam da publicidade de dados pessoais serão fundamentadas nos arts. 3º e 31 da LAI, considerando:

I - a especificidade da LAI em relação ao Poder Público para regular aspectos de transparência e acesso à informação;

II - o não estabelecimento, pela LGPD, de hipóteses de sigilo para a Administração Pública e nem contra esta; e

III - a restrição do acesso a quaisquer dados pessoais relativos à intimidade, vida privada, honra e imagem das pessoas, nos termos do art. 31 da LAI.

Parágrafo único. A aplicação da LAI e da LGPD deve ocorrer de forma integrada, tendo por premissa a compatibilidade entre os comandos legais.

CAPÍTULO IV

DA TRANSFERÊNCIA E DO COMPARTILHAMENTO DE DADOS NO CFF

Art. 9º. O CFF poderá transferir dados pessoais constantes de suas bases de dados a pessoas jurídicas de direito privado nos seguintes casos, sem prejuízo de outros previstos em legislação específica:

I - de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI;

II - em que os dados forem acessíveis publicamente, observadas a finalidade, a boa-fé e os direitos do titular;

III - em que houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, bem como, em caso de transferência internacional de dados, sejam observadas as disposições do art. 33 e seguintes da Lei Federal nº 13.709/2018; ou

IV - em que a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou a proteção e o resguardo da segurança e da integridade do titular dos dados, sendo vedado o tratamento para outras finalidades.

Parágrafo único. A pessoa jurídica de direito privado receptora dos dados pessoais será qualificada como operadora, consoante o estabelecido no art. 5º, inciso VII da LGPD.

Art. 10. O compartilhamento de dados pessoais com outras instituições públicas observará o disposto na legislação vigente e em regulamentação específica do CFF.

CAPÍTULO V

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Art. 11. O controlador de dados pessoais, nos termos do art. 5º inciso VI da LGPD, é o Conselho Federal de Farmácia e os Conselhos Regionais de Farmácia nas hipóteses de captação de dados dispostas na Política de Privacidade e Segurança da Informação do CFF.

Art. 12. É operador, nos termos do art. 5º inciso VII da LGPD, no âmbito do CFF, a pessoa natural ou jurídica, de direito público ou privado, que realizar tratamento de dados pessoais em nome do CFF.

Parágrafo único. Não é considerado operador, para os fins desta Política, a pessoa física com vínculo empregatício ou a pessoa jurídica controladora do dado, tais como autoridades, conselheiros e colaboradores do CFF.

Art. 13. Os fornecedores de produtos ou serviços, ao tratarem os dados pessoais a eles confiados pelo CFF, serão considerados operadores e deverão submeter-se à Política estabelecida por este normativo, cumprir os deveres e obrigações legais e contratuais aplicáveis, além de:

I - assinar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais definidas pelo CFF;

II - apresentar evidências e garantias suficientes de que aplicam medidas técnicas e administrativas adequadas de segurança para a proteção dos dados pessoais, nos termos definidos em legislação, em normas administrativas do CFF e nos respectivos instrumentos contratuais;

III - manter os registros de tratamento de dados pessoais que realizarem, de forma a oferecer condições de rastreabilidade e a fornecer prova eletrônica a qualquer tempo;

IV - seguir fielmente as diretrizes e instruções transmitidas pelo CFF;

V - facultar acesso a dados pessoais somente para pessoas que tenham obtido autorização, a qual será concedida apenas a quem tenha estrita necessidade de conhecer tais dados e que tenha assumido compromisso formal de preservar a segurança dos dados, devendo a prova do compromisso estar disponível em caráter permanente para exibição ao CFF, mediante solicitação;

VI - permitir a realização de auditorias e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII - auxiliar, sempre que demandado pelo CFF, no atendimento pelo respectivo contratante, de obrigações perante titulares de dados pessoais, autoridades competentes ou quaisquer outros interessados com previsão legal;

VIII - comunicar formalmente e de imediato ao encarregado do CFF a ocorrência de qualquer incidente de segurança que possa acarretar risco, comprometimento ou dano potencial ou efetivo ao titular de dados pessoais; e

IX - descartar de forma irrecuperável, ou devolver para o contratante, todos os dados pessoais e as respectivas cópias existentes, após o cumprimento da devida finalidade ou após o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Art. 14. O encarregado de dados do CFF atuará como canal de comunicação entre o CFF, os titulares dos dados e a ANPD, bem como com outras organizações com atuação na proteção de dados pessoais com as quais o CFF estabeleça acordo de serviço ou de cooperação técnica, sendo indicado pelo presidente do CFF.

Art. 15. Ao encarregado, compete:

I - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar as providências cabíveis;

II - receber comunicações da Autoridade Nacional e adotar providências cabíveis;

III - orientar autoridades, servidores e colaboradores do CFF a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo CFF ou estabelecidas em normas complementares.

Parágrafo único. A orientação prevista no inciso III do caput deste artigo será considerada de natureza técnica e publicada internamente de forma permanente e cumulativa.

CAPÍTULO VI

DA SEGURANÇA E DAS BOAS PRÁTICAS

Art. 16. O CFF implementará 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 qualquer forma de tratamento inadequado ou ilícito, nos termos do capítulo VII da LGPD, por meio, no mínimo, de:

I - plano de resposta a incidentes relacionados à proteção de dados pessoais;

II - adoção de mecanismos de segurança e proteção de dados;

III - avaliação dos sistemas e dos bancos de dados em que houver tratamento de dados pessoais;

IV - análise da segurança quando do compartilhamento de dados pessoais com terceiros;

V - registro e manutenção dos tratamentos de dados pessoais com as informações sobre finalidade do tratamento, base legal, descrição dos titulares, eventual transferência internacional, prazo de conservação e medidas de segurança adotadas;

VI - guarda dos dados pessoais, fundamentada na tabela de temporalidade;

VII - instituição de órgão colegiado como instância técnica para tratar de assuntos relativos à segurança da informação e proteção de dados pessoais; e

VIII - utilização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como auxílio à tomada de decisão e proteção de dados pessoais.

Art. 17. O CFF adotará regras de boas práticas e governança em segurança da informação, com a finalidade de orientar comportamentos adequados e mitigar os riscos de comprometimento dos dados pessoais tratados nas atividades de controle externo e administrativas do Conselho.

CAPÍTULO VII

DA INTERAÇÃO COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Em caso de incidente de segurança que envolva dados pessoais e que possa acarretar risco ou dano relevante aos titulares, será priorizada a contenção do incidente e a ANPD será informada no prazo estipulado pela Autoridade Nacional.

§ 1º A comunicação 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;

IV - os riscos relacionados ao incidente; e

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

§ 2º A comunicação será realizada pelo presidente do CFF, após proposta do encarregado de dados.

CAPÍTULO VIII

Considerações Finais

Art. 19. O CFF deverá reforçar e aprimorar constantemente a Política estabelecida por esta Portaria, empreendendo estudos para verificar a necessidade de sua revisão, anualmente, em observância à evolução tecnológica, jurisprudencial, regulatória e aos novos paradigmas de boas práticas.

Parágrafo único. As boas práticas adotadas para a proteção de dados pessoais e a governança implantada deverão ser objeto de campanhas informativas, a fim de disseminar a cultura protetiva e de transparência, com conscientização e sensibilização dos interessados.

Art. 20. Na aplicação de procedimentos, orientações e normativos em situações que impactem o tratamento de dados pessoais, devem ser observados os princípios e diretrizes aplicáveis para o tratamento de dados pessoais.

Art. 21. Caso a ANPD, no exercício de suas competências legais, preveja prazos diversos dos estabelecidos nesta Portaria, prevalecerão aqueles definidos pela Autoridade Nacional.

Art. 22. Os casos omissos serão resolvidos pelo Comitê de Privacidade e Proteção de Dados do CFF.

Art. 23. Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Walter da Silva Jorge João**, **Presidente do Conselho Federal de Farmácia**, em 12/12/2025, às 17:56, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida clicando **aqui** informando o código verificador **0930683** e o código CRC **498B072B**.

ANEXO ÚNICO

POLÍTICA DE PRIVACIDADE E SEGURANÇA DO CONSELHO FEDERAL DE FARMÁCIA

1. OBJETIVO

A presente política tem como objetivo definir as diretrizes para a privacidade e o tratamento de dados em conformidade com a Lei Geral de Proteção de Dados, em cumprimento ao disposto no inciso I, art. 23.

Além disso, estabelece as diretrizes de segurança da informação para o Conselho Federal de Farmácia (CFF), com foco na proteção da confidencialidade, integridade e disponibilidade dos dados. Essas diretrizes buscam assegurar que todas as atividades sejam realizadas de maneira segura, correta, ética e legal por todos os colaboradores.

2. ABRANGÊNCIA

Esta política abrange todos os conselheiros, colaboradores, prestadores de serviços, convidados e terceiros envolvidos nas atividades do Conselho Federal de Farmácia, tanto nas operações internas quanto externas, sejam realizadas de forma presencial ou virtual.

3. REFERÊNCIAS

Lei Geral de Proteção de Dados – Lei nº 13.709/2018
ABNT NBR ISO/IEC 27001 – Requisitos do Sistema de Gestão de Segurança da Informação – 2006;

4. DEFINIÇÕES E SIGLAS

Colaboradores: todas as pessoas que atuam direta ou indiretamente em nome do CFF, ou seja, diretores, gestores, empregados, estagiários, ou quaisquer pessoas que possam atuar em nome da entidade.

Confidencialidade: propriedade de manter a informação a salvo de acesso e divulgação não autorizados, devendo ser observados as disposições do Regulamento Interno de Segurança da Informação - RISI do CFF.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade determinada e previamente descrita.

Conta de Acesso ou User ID: símbolo ou sequência de caracteres usados por um sistema para identificar um usuário específico de forma a garantir sua unicidade.

Correio eletrônico ou e-mail: é a composição, transmissão e armazenagem de mensagens e arquivos entre usuários de sistemas de rede. Sendo transmitido via quaisquer meios eletrônicos como por exemplo por meio de protocolos de correio tais como SMTP (*Simple Mail TransferProtocol*), POP (*Post Office Protocol*) ou IMAP (*Internet Message Access Protocol*).

CRF: Conselho Regional de Farmácia. Estão presentes em todo o território nacional, abrangendo todos os estados da federação, incluindo o Distrito Federal.

Criptografia: ciência que se dedica a transcrever dados em cifras ou códigos que poderão ser, teoricamente, lidos apenas pelo destinatário da informação.

Dados pessoais: são todas as informações que permitem a identificação de uma pessoa natural, como por exemplo: CPF, e-mail, nome, telefone, entre outros.

Dados pessoais sensíveis: são dados pessoais relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.

Disponibilidade: situação de manter a informação acessível, quando necessário, ou seja, situação que os dados possam ser consultados.

Dispositivos móveis: dispositivo utilizado para transmitir e/ou armazenar dados e informações de forma eletrônica, por exemplo: CDs/DVDs, Blu-ray, pen drives, HD externo, Smartphones, Tablets, entre outros.

Documentos especiais: refere-se a qualquer documento físico que contenha informações pessoais identificáveis, conforme definido pela LGPD. Isso inclui, mas não se limita a registros financeiros, documentos de identificação, documento pessoal de colaborador, entre outros.

Gestor da informação: responsável pela informação e medidas necessárias à segurança e controle efetivo do acesso à informação.

Hardware: unidades físicas, componentes, circuitos integrados, discos e mecanismos que compõem um computador ou os seus periféricos.

Incidente de segurança: qualquer evento que resulte ou possa vir em resultarem perda ou dano de um ou mais atributos da informação, confidencialidade, integridade e/ou disponibilidade, ou uma violação à presente política.

Informação: no presente contexto, é tudo o que se sabe sobre as atividades, propriedade ou inteligência do CFF e dos CRFs, seja de conhecimento de pessoas ou que estejam presentes em equipamentos de TI, papéis ou em quaisquer outros meios de armazenamento, transmissão ou processamento.

Informação ostensiva: aquela cujo acesso pode ser franqueado por qualquer pessoa, sem restrição.

Informação interna: é uma informação cujo conhecimento e uso está no âmbito interno do CFF, estando disponível a todos os colaboradores, bem como a fornecedores e prestadores de serviço que possuam cláusula de confidencialidade assinadas nos contratos de prestação de serviço.

Informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e Estado. O acesso deve ser restrito às pessoas que, por seu cargo ou função, tenham necessidade de tomar conhecimento do seu teor.

Integridade: propriedade de manter a informação exata, completa e atualizada.

LGPD: Lei Federal n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

Prestadores de serviços: pessoa ou empresa que presta serviços à organização em atividades de curta ou média duração, incluindo consultores externos, terceiros, auditores externos entre outros.

Rede wireless: uma rede wireless ou sem fio refere-se a uma passagem aérea sem a necessidade do uso de cabos por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho. Incluem, mas não se limitam a equipamentos Wi-Fi e Bluetooth.

Segregação de funções (*SOD SegregationOfDuties*): consistem na separação entre pessoas distintas das atividades conflitantes de execução, autorização, aprovação, contabilização e controle, objetivando a redução da incidência de falhas ou fraudes, independentemente se sua estruturação é automática ou não.

Software: qualquer programa ou grupo de programas que instrui ao hardware sobre a maneira como ele deve executar uma tarefa, inclusive sistemas operacionais, processadores de texto e programas de aplicação.

Termo de consentimento: documento que coleta manifestação favorável ao tratamento dos dados pessoais para finalidades específicas e determinadas.

TI: Tecnologia da Informação.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento de dados pessoais: significa qualquer operação, como 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, realizada com dados pessoais.

RISI: Regulamento Interno de Segurança da Informação do Conselho Federal de Farmácia.

5. DIRETRIZES DA PRIVACIDADE E TRATAMENTO DE DADOS PESSOAIS

5.1. Segurança da Informação

A preservação e proteção adequadas das informações são essenciais para o sucesso das missões do Conselho Federal de Farmácia. As informações podem surgir de várias formas, como impressas, eletrônicas, transmitidas por diferentes meios ou comunicadas verbalmente. Independentemente de sua forma ou meio de transmissão, garantir a segurança dessas informações é fundamental.

A segurança da informação envolve a proteção contra diversas ameaças para assegurar a continuidade e eficácia das atividades. Isso demanda a implementação de controles, incluindo políticas, processos, estruturas organizacionais e tecnologias, além da construção, preparação, monitoramento e análise crítica desses mecanismos de proteção.

Assim, esta diretriz serve como o principal guia para direcionar e orientar as iniciativas de segurança da informação no CFF, além de estabelecer procedimentos que atendam aos requisitos legais e às necessidades da entidade.

Ao adotar essas diretrizes, busca-se mitigar os riscos relacionados à segurança dos dados e informações, e todos os colaboradores devem seguir as orientações estabelecidas nesta política ao realizar procedimentos e atividades. Embora baseadas nas normas estabelecidas neste texto poderão ser elaboradas políticas complementares, tal qual como a observância ao Regulamento Interno de Segurança da Informação do CFF - RISI.

Nesse sentido, são ações realizadas pelo CFF, com a finalidade de garantir a proteção dos dados pessoais, mas não se limitando a:

Controle de acesso: estabelecer normas para a gestão do acesso aos principais sistemas do CFF, incluindo padrões de senha e perfis de acesso.

Desenvolvimento seguro: definir diretrizes de segurança da informação relacionadas à aquisição, desenvolvimento e manutenção de sistemas e aplicações de negócios.

Segurança da informação em infraestrutura de tecnologia: determinar requisitos para uma operação segura, formal, monitorada e adequada dos recursos de TI, incluindo padrões de configuração segura

para a instalação de hardware, software e aplicativos, conforme disposição do Regulamento Interno de Segurança da Informação do CFF - RISI.

Gestão de incidentes de segurança: revisar procedimentos para a resposta a eventos de segurança da informação, permitindo a tomada de ações corretivas.

Gestão do antivírus: regular a administração, proteção e tratamento contra softwares, programas ou scripts maliciosos.

Gestão de firewall e VPN: estabelecer regras para concessão de acesso, abrangendo colaboradores, clientes, terceiros, parceiros, prestadores de serviços, entidades estatais e outros.

Controle de dispositivos móveis: definir regras para o controle e proteção de dispositivos móveis, bem como para a autorização de uso de equipamentos de terceiros dentro das instalações do CFF.

Uso do correio eletrônico: regular o uso seguro e apropriado do e-mail corporativo, incluindo suas restrições de utilização.

Gestão da rede wireless: definir as regras para o uso da rede sem fio, garantindo acesso à rede interna apenas para pessoas e equipamentos autorizados.

Uso da internet: estabelecer regras para a liberação de acesso à internet de acordo com perfis predefinidos, respeitando as normas do CFF.

Monitoramento de acessos: definir diretrizes e procedimentos para o monitoramento periódico de ações críticas ou realizadas por usuários privilegiados em sistemas selecionados, de acordo com a criticidade para o CFF.

Além das ações acima mencionadas, esta diretriz também estabelece que:

(i) todas as informações e documentos criados, armazenados, transmitidos e/ou processados no CFF, tanto em formato físico quanto eletrônico, são de propriedade ou estão sob a custódia da entidade. A divulgação total ou parcial desses dados sem a devida autorização das áreas responsáveis é proibida. Os gestores são responsáveis por garantir que seus colaboradores cumpram esta diretriz;

(ii) o CFF pode automaticamente coletar e armazenar informações sobre as atividades de qualquer colaborador que utilize seus recursos, incluindo, mas não se limitando a endereços de rede dos equipamentos, identificadores de usuário, aplicativos utilizados, páginas ou telas acessadas e conversas realizadas por meio dos recursos da organização;

(iii) prestadores de serviço e demais terceiros também devem seguir as políticas internas do CFF, bem como as disposições do “Termo de Confidencialidade” firmado no momento da contratação, conforme a necessidade. Em caso de uso inadequado ou descumprimento das normas, serão responsabilizados nos termos acordados.

(iv) qualquer acesso privilegiado a sistemas e informações do CFF realizado por prestadores de serviço deve ser aprovado previamente pelo Comitê de

Privacidade e Proteção de Dados;

(v) é proibido para todos os usuários usar ou tentar acessar qualquer sistema ou aplicativo sem a devida autorização formal.

Questões ou solicitações de informações adicionais sobre normas complementares e regras técnicas relacionadas à Segurança da Informação podem ser enviadas para o e-mail ti@cff.org.br.

a) Classificação da Informação

As informações pertencentes ou sob a responsabilidade do CFF devem ser identificadas, utilizadas, armazenadas, transmitidas e descartadas de acordo com sua classificação, a qual é formalmente atribuída pelo responsável pela gestão da informação. É estritamente proibido que os colaboradores façam uso inadequado das informações do Conselho, compartilhem-nas, as utilizem para benefício pessoal ou armazenem arquivos e e-mails de maneira imprópria. Os gestores devem assegurar que essas diretrizes sejam cumpridas por seus colaboradores.

O acesso às informações é restrito apenas a pessoas autorizadas. As informações podem ser reclassificadas conforme necessário e de acordo com os prazos de validade descritos em normas específicas, devendo o nível de proteção ser ajustado à sua classificação atual.

As informações, conforme seu nível de classificação, deverão ser submetidas aos seguintes controles:

Ostensiva: aquela cujo acesso pode ser franqueado a qualquer pessoa, sem restrição.

Informação interna: é uma informação cujo conhecimento e uso está no âmbito interno do CFF, estando disponível a todos os colaboradores, bem como a fornecedores e prestadores de serviço que possuam cláusula de confidencialidade assinadas nos contratos de prestação de serviço.

Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. O acesso deve ser restrito às pessoas que, por seu cargo ou função, tenham necessidade de tomar conhecimento do seu teor.

5.2 Coleta e utilização dos dados

a) Fontes dos Dados Pessoais.

O CFF somente coleta ou recebe, através da consecução de sua missão institucional, dados pessoais quando:

(i) do recebimento dos dados profissionais coletados pelos Conselhos Regionais de Farmácia, os quais são encaminhados ao Conselho Federal de Farmácia;

(ii) em hipóteses de admissão de funcionários e registro de imagem para fins de controle de acesso de pessoal;

(iii) quando da inscrição de profissionais em cursos, palestras, capacitações e congêneres;

(iv) quando da inserção de dados em sítios eletrônicos, softwares e plataformas vinculadas ao CFF;

(v) em contratações de prestações de serviços ou contratação com terceiros;

(vi) em convocações, ordens de serviço, relatórios de prestação de contas e demais documentos oficiais em que sejam necessários dados pessoais.

b) Principais finalidades para tratamento de Dados Pessoais.

Os tipos de dados pessoais e suas finalidades variam conforme a atividade em questão, como, por exemplo, no âmbito da prestação de serviços, na fiscalização da profissão, nas contratações efetuadas pelo Conselho, e na sua atuação educativa. Isso também abrange o acesso a plataformas para transferência de dados internas e externas. Os dados coletados são mantidos em sigilo e podem ser usados pelo CFF em suas finalidades institucionais.

c) Dados Pessoais coletados pelos Conselhos Regionais e Federal de Farmácia

Os Dados Pessoais coletados dos profissionais inscritos incluem os itens listados a seguir, que podem mudar conforme o serviço solicitado, a Plataforma empregada ou a atividade realizada.

c.1) Dos dados coletados pelos Conselhos Regionais e encaminhados ao Conselho Federal de Farmácia:

(i) informações de cadastro: número de inscrição, nome, CPF, endereço, data de nascimento, filiação, naturalidade, RG, título de eleitor com zona e seção, estado civil, certificado militar, grupo sanguíneo, doador ou não doador de órgãos, diploma e histórico escolar, imagem da biometria, e-mail, telefone e habilitações profissionais.

c.2) Dos dados coletados diretamente pelo Conselho Federal de Farmácia:

(i) informações de cadastro: nome, CPF, endereço, telefone, e-mail, assinatura e outras informações que possam ser exigidas conforme a atividade;

(ii) informações sobre dispositivos: endereço IP, data e hora de acesso à plataforma (se aplicável), localização geográfica, origem de referência, tipo de navegador, duração da visita e páginas acessadas;

(ii) informações financeiras: dados bancários (incluindo banco, agência e número da conta);

(iv) dados de gravação: registros de voz e imagem quando necessários para o cumprimento das atividades do CFF.

d) Compartilhamento e Transferência de Dados

Durante a consecução das atividades, os dados pessoais podem ser compartilhados:

1. Entre o Conselho Federal de Farmácia e os Conselhos Regionais, dentro do âmbito de suas competências.

2. Com prestadores de serviços e contratados pelo CFF, como aqueles responsáveis pela manutenção de sistemas e equipamentos, serviços de nuvem, cobrança de valores devidos, e serviços jurídicos, entre outros.

3. Com autoridades judiciais, administrativas ou governamentais competentes, quando houver uma determinação legal, solicitação fundamentada na Lei Federal 13.709/18, ou ordem judicial.

4. Com base no art. 7º da Lei Geral de Proteção de Dados, após verificação da relevância e legalidade pelo Comitê de Privacidade e Proteção de Dados.

Não será autorizada a divulgação de dados pessoais dos usuários para fins diversos dos previstos nesta política, exceto nas hipóteses legalmente previstas na LGPD, bem como após a aprovação pelo Comitê de Privacidade e Proteção de Dados do Conselho Federal de Farmácia. Nesses casos, serão adotadas todas as medidas necessárias para assegurar que os dados sejam tratados de maneira confiável, segura e em conformidade com a LGPD.

e) Direitos e deveres dos usuários com relação aos Dados Pessoais

De acordo com a Lei Geral de Proteção de Dados (Lei 13.709/2018 -LGPD), o usuário possui os seguintes direitos, dentro da competência de cada um dos Conselhos:

(i) confirmar que seus dados pessoais estão sendo tratados;

(ii) acessar seus dados pessoais;

(iii)corrigir dados pessoais que estejam incompletos, incorretos ou desatualizados;

(iv) anonimizar, bloquear ou eliminar dados pessoais que sejam desnecessários, excessivos ou tratados em desacordo com a LGPD;

(v) excluir os dados pessoais tratados com base em seu consentimento, exceto nas situações de retenção de Dados Pessoais previstas na LGPD;

(vi) obter informações sobre o compartilhamento dos dados pessoais;

(vii) receber informações sobre a possibilidade de não fornecimento de consentimento;

(viii) revogar o consentimento para o tratamento dos dados pessoais, quando se tratar desta hipótese;

(ix) opor-se a qualquer tratamento que infrinja a LGPD.

São deveres do usuário:

(i) fornecer informações precisas e assumir a responsabilidade por quaisquer consequências decorrentes de erros e omissões;

(ii) cumprir as diretrizes estabelecidas nesta Política de Privacidade;

(iii) assumir a responsabilidade pelo uso de dados pessoais por aplicativos de terceiros em seus dispositivos;

(iv) garantir a segurança do dispositivo utilizado para acessar o serviço.

É possibilitado ao usuário exercer quaisquer dos direitos acima enviando um e-mail para: dpo@cff.org.br . Ressaltando que antes de ser apresentada qualquer solicitação para exercício dos direitos mencionados

acima, fica reservado ao CFF solicitar ao usuário o fornecimento de algumas informações para confirmação de identidade.

f) Sobre o Tratamento de Dados de Menores de Idade

No que diz respeito ao tratamento de dados de menores de idade, este ocorrerá exclusivamente dentro do Programa de Educação em Saúde na Pediatria (Cacilda, Saúde e CIA). A coleta de dados de menores de 18 anos apenas será realizada mediante consentimento prévio e formal dos pais ou responsáveis legais. Tais dados serão devidamente protegidos, garantindo-se a preservação da privacidade do menor.

g) Armazenamento e proteção dos dados pessoais.

O armazenamento dos dados pessoais é realizado de maneira segura em sistemas terceirizados do CFF, seguindo as exigências legais. São aplicadas as melhores práticas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, divulgação ou qualquer tipo de tratamento inadequado ou ilegal. As seguintes medidas de segurança de dados são implementadas:

(i) acesso limitado aos sistemas e bases de dados;

(ii) restrição ao acesso a sites e softwares dentro das instalações do Conselho;

(iii) utilização de ferramentas e realização de testes de segurança para assegurar o cumprimento das medidas de proteção de dados;

(iv) monitoramento dos acessos e das atividades relacionadas aos dados pessoais.

É importante destacar que o CFF não se responsabiliza pela coleta de dados ou por problemas relacionados ao sistema do equipamento do usuário (como vírus, ataques de hackers, abuso de uso, ou vulnerabilidades do sistema do dispositivo, entre outros). Portanto, recomendamos tomar precauções de como utilizar equipamentos e conexões seguras e manter seu antivírus atualizado.

Além disso, como nenhum sistema é totalmente infalível, caso identifique qualquer falha ou violação, por favor, comunique-nos pelo e-mail dpo@cff.org.br para que possamos adotar as medidas necessárias.

Também é possível contato pelos telefones (61) 3878-8700 ou pessoalmente no endereço SHIS - Setor de Habitações Individuais Sul, Lote L, s/n QI 15 - Lago Sul, Brasília - DF, 71635-615. Correspondências podem ser enviadas para o mesmo endereço.

h) Consentimento do usuário para autorização do uso de dados.

A LGPD define várias situações em que o tratamento de dados pessoais é permitido sem a necessidade do consentimento do titular, conhecidas como "bases legais para o tratamento de dados".

Isso significa que, ao usar as plataformas e os serviços, pode ser possível coletar e processar dados sem obter consentimento, desde que haja uma base legal estabelecida pela LGPD que permita isso. Essas bases podem incluir a execução de contratos, proteção à saúde, cumprimento de obrigações legais ou regulatórias, exercício regular de direitos e interesses legítimos.

Quando o tratamento se basear no "consentimento", será solicitado um consentimento específico para o tratamento dos dados pessoais dos usuários.

5.3 Tratamento e descarte de dados pessoais e documentos sensíveis

Para proteger a privacidade dos dados pessoais, adotamos medidas rigorosas em nossas plataformas e serviços para garantir que as informações pessoais não sejam armazenadas por mais tempo do que o necessário. Isso significa que os dados pessoais são conservados pelo CFF somente pelo período necessário para cumprir as finalidades institucionais, obrigações legais ou regulatórias ou para exercer nossos direitos de maneira adequada.

Vale ressaltar que, após o período necessário para as finalidades específicas, os dados podem ser retidos de forma anonimizada, ou seja, sem a possibilidade de serem vinculados diretamente ao titular. Isso permite a manutenção dos dados por períodos mais longos sem comprometer a privacidade dos usuários.

a) Anonimização e descarte de dados e documentos

A destruição e a anonimização dos dados devem ser efetuadas de acordo com os procedimentos estabelecidos pela área de segurança da informação. No entanto, em todos os casos, devem ser seguidos os seguintes procedimentos:

(i) identificação dos locais de armazenamento;

(ii) descarte de dados pessoais em ambientes físicos e digitais: quando for necessário descartar informações, isso deve ser feito de maneira que impeça a reconstrução dos dados, seja no ambiente físico ou digital;

(iii) antes de descartar dados pessoais que não estejam contidos em documentos oficiais e, portanto, não estejam submetidos à tabela de temporalidade, o gestor do departamento responsável pelo tratamento, em conjunto com o encarregado, deve aprovar o descarte;

(iv) registro de descarte: recomenda-se manter um registro das operações de descarte de documentos.

b) Com relação aos documentos físicos contendo dados pessoais:

Observe que os registros em papel que NÃO CONTENHAM dados pessoais, informações financeiras ou informações confidenciais podem ser eliminados por meio de reciclagem, trituração, descarte no lixo comum ou destruição física, conforme considerado adequado.

Por outro lado, os registros em papel que CONTENHAM dados pessoais, informações financeiras ou informações confidenciais devem ser triturados e descartados em lixo específico.

Além disso, todos os colaboradores devem estar informados sobre o procedimento de descarte de documentos para garantir a eficácia desta política.

5.4 Divulgação de dados internos

A proteção dos dados é uma prioridade para o CFF, e para assegurar sua integridade e segurança, são estabelecidas diretrizes rigorosas em várias áreas da gestão da informação.

Para isso, qualquer compartilhamento de informações internas com terceiros e contratados deve ser formalizado por meio de cláusulas contratuais específicas, conforme um modelo previamente definido

pela Coordenação de Consultoria Jurídica do CFF. Isso assegura a manutenção consistente dos padrões de confidencialidade em todas as interações com partes externas.

A proteção das informações vai além de sua divulgação e cobre todo o ciclo de vida dos dados, desde a sua criação até a sua destruição. É essencial garantir a proteção adequada para evitar qualquer comprometimento da confidencialidade dos dados.

Durante o armazenamento físico, documentos e mídias contendo informações devem ser guardados em locais seguros, como cofres ou arquivos trancados, e cópias de segurança devem ser mantidas em instalações externas para proteção adicional.

A impressão de informações internas também requer controles rigorosos, como o uso de capas e pastas para evitar perdas. Essas medidas ajudam a garantir a rastreabilidade e integridade dos documentos impressos.

No ambiente digital, a criptografia é crucial para proteger as informações internas. Durante o armazenamento e a transmissão, os dados podem ser criptografados usando protocolos específicos para garantir sua segurança.

Assim, o CFF adota uma abordagem abrangente e proativa para a proteção de informações, implementando medidas e controles rigorosos em todas as etapas de seu ciclo de vida, desde a criação até a destruição. Essas práticas demonstram o compromisso da organização com a segurança da informação e a proteção de seus interesses.

5.5. Proibição de acesso

Não é permitido acessar, copiar ou armazenar programas de computador ou qualquer outro material que infrinja a lei de direitos autorais, bem como conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista ou que faça apologia ao crime. Além disso, é proibido utilizar os recursos computacionais ou qualquer outro recurso do CFF, fornecido ao colaborador para o desempenho de suas funções, para constranger, assediar, prejudicar ou ameaçar indivíduos ou organizações. Também é vedado se passar por outra pessoa ou ocultar a própria identidade ao usar os recursos do CFF.

5.6 Licenciamento

Todo software utilizado nos equipamentos da rede interna do CFF deve ser devidamente licenciado; a utilização de qualquer software sem licença é proibida.

Para utilizar softwares livres ou temporários, é necessário fazer uma solicitação por meio de um chamado à Coordenação de Tecnologia da Informação. Se aprovado, a instalação e remoção desses softwares deverão ser realizadas pelo próprio setor.

O uso de softwares não licenciados é considerado uma prática inadequada e resultará em sanções para o colaborador ou terceiro vinculado ao CFF. É importante destacar que tal prática, conhecida como "pirataria", está sujeita a penalidades conforme a legislação vigente.

5.7. Sanções e Penalidades

É responsabilidade do colaborador informar imediatamente à área de segurança da informação sobre qualquer violação desta política ou qualquer conduta que possa afetar o funcionamento normal da rede, sistemas, processos ou operações do CFF, seja de forma intencional ou não.

É importante destacar que o não cumprimento das políticas e normas do CFF pode resultar em sanções conforme a legislação vigente.

Qualquer uso não autorizado ou tentativa de uso não autorizado de credenciais e senhas para acessar ativos, serviços de informação ou recursos computacionais será tratado como um incidente de segurança, com a aplicação de penalidades adequadas.

Nos casos de violação de regras que não estejam especificamente cobertas por esta política, serão implementadas medidas educativas. Essas medidas serão discutidas com o superior imediato do colaborador ou o gestor responsável pelo contrato relacionado, com o objetivo de corrigir o comportamento e assegurar a conformidade com as políticas da organização.

6.DISPOSIÇÕES FINAIS

Esta política deve ser revisada anualmente ou sempre que houver mudanças substanciais nas diretrizes de segurança da informação. O objetivo é garantir que a política permaneça atualizada em relação às evoluções tecnológicas, processos e às necessidades da instituição e segurança da informação e deve ser publicizada a todos os interessados.