

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS DA SAÚDE
PROGRAMA DE PÓS-GRADUAÇÃO EM ODONTOLOGIA

**LEI GERAL DE PROTEÇÃO DE DADOS:
ADEQUAÇÕES DOS SERVIÇOS ODONTOLÓGICOS
NO BRASIL**

Manoel Pereira de Lima

SAPIENTIA AEDIFICAT

MANOEL PEREIRA DE LIMA

**LEI GERAL DE PROTEÇÃO DE DADOS: ADEQUAÇÕES DOS
SERVIÇOS ODONTOLÓGICOS NO BRASIL**

**GENERAL DATA PROTECTION LAW: ADJUSTMENTS OF
DENTAL SERVICES IN BRAZIL**

Dissertação apresentada ao Programa de Pós-Graduação em Odontologia, da Universidade Federal da Paraíba, como parte dos requisitos para obtenção do título de Mestre em Odontologia – Área de Concentração em Ciências Odontológicas.

Orientador: Prof. Dr. Marcelo Augusto Oliveira de Sales

João Pessoa

2023

Catálogo na publicação
Seção de Catalogação e Classificação

L732l Lima, Manoel Pereira de.

Lei geral de proteção de dados : adequações dos
serviços odontológicos no Brasil / Manoel Pereira de
Lima. - João Pessoa, 2023.

50 f. : il.

Orientação: Marcelo Augusto Oliveira de Sales.
Dissertação (Mestrado) - UFPB/CCS.

1. Odontólogos. 2. Privacidade - Informação. 3.
Segurança computacional. 4. Lei - Aplicação. 5.
Confidencialidade - Informação. I. Sales, Marcelo
Augusto Oliveira de. II. Título.

UFPB/BC

CDU 616.314-051(043)



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS DA SAÚDE
PROGRAMA DE PÓS-GRADUAÇÃO EM ODONTOLOGIA



ATA DA DEFESA PÚBLICA DE DISSERTAÇÃO DE MESTRADO
2023

Aos quinze dias do mês de fevereiro do ano de 2023, às 09:00 com uso de recursos a distância, reuniram-se os membros da banca examinadora composta pelas professores doutores: MARCELO AUGUSTO OLIVEIRA DE SALES (Orientador e Presidente), EDSON HILAN GOMES DE LUCENA (membro interno ao Programa de Pós-graduação em Odontologia – UFPB) e MANUEL ANTONIO GORDON NUNEZ (membro externo ao Programa de Pós-graduação em Odontologia – UFPB) a fim de arguirem o(a) mestrando(a) MANOEL PEREIRA DE LIMA, com relação ao seu trabalho final de curso de mestrado (dissertação), sob o título “LEI GERAL DE PROTEÇÃO DE DADOS: ADEQUAÇÕES DOS SERVIÇOS ODONTOLÓGICOS NO BRASIL”. Aberta a sessão pelo presidente da mesma, coube o(a) candidato(a), na forma regimental, expor o tema de sua dissertação, dentro do tempo regulamentar. Em seguida, foi questionado pelos membros da banca examinadora, sendo as explicações necessárias fornecidas e as modificações solicitadas registradas. Logo após, os membros da banca examinadora reuniram-se em sessão secreta, tendo chegado ao seguinte julgamento, que, de público, foi anunciado: 1º Examinador (membro externo): Conceito “Aprovado”; 2º Examinador (membro externo): Conceito “Aprovado, 3º Examinador (Orientador e presidente): Conceito “Aprovado”. O que resultou em conceito final igual: “APROVADO”, o que permite o(a) candidato(a) fazer jus ao título de Mestre em Odontologia. Os documentos utilizados para avaliação da candidata durante o processo aqui descrito apresentam-se como prova documental do mesmo e, como tal, serão anexadas a esta ata para arquivamento. Nada mais havendo a tratar, foi lavrada a presente ata, que será assinada pelo presidente, pelos demais membros da banca e pelo(a) candidato (a).

1º Examinador – Membro Externo

2º Examinador – Membro Interno

Documento assinado digitalmente
gov.br MARCELO AUGUSTO OLIVEIRA DE SALES
Data: 26/02/2023 09:50:49-0300
Verifique em <https://verificador.iti.br>

3º Examinador – Presidente

Documento assinado digitalmente
gov.br MANOEL PEREIRA DE LIMA
Data: 26/02/2023 19:23:14-0300
Verifique em <https://verificador.iti.br>

Candidato (a)

DEDICATÓRIA

Dedico a Deus, antes de qualquer coisa. Sem Ele eu não teria a capacidade de me levantar todas as vezes em que tropecei. Mas dedico também a minha mãe e ao meu irmão, por serem combustível na estrada em que sonhamos, juntos.

AGRADECIMENTOS

A Deus, por toda força e discernimento durante esse percurso, pela graça de me ter feito chegar até, sempre me aparando quando eu mais precisava.

À minha família, em especial minha mãe, Marli, que sempre tão forte e guerreira me ensinou as matérias mais importantes para a vida: simplicidade, coragem, amor e verdade. Sem ela eu nada seria, a ela toda a minha gratidão e orgulho em tê-la como mãe. À minha avó e meu irmão, que nunca soltaram a minha mão e me apoiaram em todas as minhas decisões, não só profissionais, mas de vida. Tudo isso é fruto da nossa união e amor.

Ao meu pai, “*In Memoriam*”, por todo ensinamento e por ser meu guia. Sei que de onde estiver, cuida de mim.

A Bríssio, que sempre me impulsionou na realização desse sonho, que acreditou que tudo daria certo, mesmo quando as situações não eram tão favoráveis. Me ensinou muito sobre a vida, sobre amor, respeito e paciência.

Aos amigos que sempre torceram por mim, em especial a Neto, que desde a graduação topou esse desafio e tantos outros junto comigo, partilhando de muito conhecimento e impulsionando nossos sonhos. Mas também às amigas que o mestrado me proporcionou conhecer, nas pessoas de Lays Gomes, Andrêzza e Yasmin, pelas quais guardo muito carinho e admiração.

Ao meu orientador, prof. Dr. Marcelo Augusto Oliveira de Sales, por todo suporte e paciência durante a escrita desse trabalho, que mesmo diante de todas as adversidades impostas a todos nós recentemente, nunca desanimou e sempre acreditou que venceríamos. Sua colaboração na minha formação será sempre lembrada com afeto.

Agradeço também aos outros tantos professores que passaram por minha vida, na pessoa da Profa. Smyrna, cada um deixando um pouco de si e fazendo com que eu me tornasse um pouco deles. Agradeço, em particular, ao prof. Manuel Gordón, a quem tenho um estimado apreço e admiração como pessoa e como profissional. O seu exemplo me motiva e me orientada na busca pelo melhor.

Ao Prof. Dr. Edson Hilan Gomes de Lucena pela disponibilidade em participar da banca e por ser tão solícito em todas as vezes que necessitei, assim como pelas contribuições dado à minha jornada acadêmica.

A minha eterna gratidão à CAPES e ao Programa de Pós-Graduação em Odontologia da UFPB, pela qualidade de ensino e por proporcionar tanto enriquecimento científico e tecnológico, demonstrando a magnitude da importância e resistência das Universidades públicas durante períodos tão difíceis e desafiadores.

Por fim, meus agradecimentos a todos que, de forma voluntária, se propuseram a responder o objeto de estudo desta pesquisa, mas em especial ao Conselho Regional de Odontologia do Estado de São Paulo e do Rio Grande do Norte, nas pessoas do Dr. Braz Antunes Mattos Neto e Dra. Karina Monney Peixoto Ferrão de Azevedo, por terem acreditado na nossa proposta de desenvolver conhecimento sobre essa temática recente e de grande valia para a nossa área de profissão.

A CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) e CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) pelo incentivo a pesquisa.

EPÍGRAFE

*“Nesse tempo de incertezas
a certeza que permanece
é que o amor é salvação
para tudo e para todos”*

Bríssio Varelo

RESUMO

Introdução: A Lei Geral de Proteção de Dados (LGPD), 13.709/2018, em vigor desde 2020, trata sobre o gerenciamento e a proteção de dados pessoais por parte de empresas, órgãos públicos e pessoa natural no Brasil, visando a garantia do direito à liberdade e à privacidade. Na saúde, assim como em outros setores, o tratamento dos dados pessoais dos pacientes deve ocorrer com o consentimento do titular e em conformidade com a nova lei. **Objetivo:** Verificar e compreender a segurança no gerenciamento de dados pessoais por parte das clínicas e consultórios odontológicos do Brasil, quanto às adequações à LGPD. **Metodologia:** Trata-se de um estudo do tipo transversal, aprovado pelo Comitê de Ética e Pesquisa – CEP (CAAE: 60717822.4.0000.5188), disponibilizado aos cirurgiões-dentistas de todo país através da plataforma *Google Forms*, por meio de um questionário estruturado. Foi definido um tamanho amostral de 374 dentistas, através do cálculo realizado na plataforma online OpenEpi (<https://www.openepi.com/>), adotando um intervalo de confiança de 95% e o efeito do desenho (deff) de 2.0. Após obtidos, os dados foram exportados e tabulados em uma planilha de Excel, e submetidos à análise no software IBM SPSS® (25.0, IBM Corporation, Armonk, New York, EUA). Procedeu-se inicialmente a análise descritiva e exploratória para determinação das frequências absolutas e relativas. Em seguida, associações estatisticamente significantes foram avaliadas por meio do teste qui-quadrado. **Resultados:** Foram obtidas 512 respostas ao questionário, evidenciando que 63,1% (n=323) dos profissionais estão vinculados somente à rede privada. Cerca de 86% (n=441) afirmaram saber o que são dados pessoais, mas 71,5% (n=366) não consegue distinguir a sua diferença entre dados pessoais sensíveis. A coleta indevida de dados pessoais de menores foi observada em 16,5% das respostas obtidas e 40,9% dos profissionais relataram disponibilizar algum termo de consentimento aos pais e/ou responsáveis. Sobre os mecanismos de segurança de dados, 72,1% relataram que o serviço estava desprotegido, não atendendo às normas da LGPD e com riscos de falhas e vazamento de informações. Observou-se, também, que 54,8% dos dentistas utilizam alguma rede social para compartilhamento de imagens de pacientes, sendo o WhatsApp a maior delas (32%). Aproximadamente 68% utilizam acesso a laudos e imagens radiográficas, através do site da clínica (28%), Idoc 49,9% e Cfaz.net (5%).

Associações estatisticamente significativas ($p \leq 0,05$) foram observadas em doze das perguntas realizadas, quando associadas à esfera administrativa. **Conclusão:** Com a realização do estudo foi possível observar que grande parte dos cirurgiões-dentistas não atende às exigências da LGPD e desconhece sua aplicabilidade dentro da odontologia, que a maioria dos serviços carece de medidas para proteção de dados e informações pessoais, bem como serviu para demonstrar a importância da lei para a sociedade, principalmente a serviços ligados à saúde.

Palavras-chave: Odontólogos; Privacidade; Segurança computacional; Aplicação da lei; Confidencialidade.

ABSTRACT

Introduction: The General Data Protection Law (GDPL), 13.709/2018, in force since 2020, deals with the management and protection of personal data by companies, public agencies and individuals in Brazil, aiming to guarantee the right to freedom and privacy. In health, as well as in other sectors, the processing of patients' personal data must occur with the consent of the holder and in accordance with the new law. **Objective:** To verify and understand the security in the management of personal data by clinics and dental offices in Brazil, regarding the adaptations to the GDPL. **Methods:** Methodology: This is a cross-sectional study, approved by the Ethics and Research Committee - ERC (CAAE: 60717822.4.0000.5188), made available to dentists throughout the country through the Google Forms platform, through a structured questionnaire. A sample size of 374 dentists was defined, through the calculation carried out on the online platform OpenEpi (<https://www.openepi.com/>), adopting a 95% confidence interval and the design effect (deff) of 2.0. After obtained, the data were exported and tabulated in an Excel spreadsheet, and submitted for analysis in the IBM SPSS® software (25.0, IBM Corporation, Armonk, New York, USA). Descriptive and exploratory analysis was initially carried out to determine absolute and relative frequencies. Then, statistically significant associations were evaluated using the chi-square test. **Results:** 512 responses to the questionnaire were obtained, showing that 63.1% (n=323) of professionals are linked only to the private network. About 86% (n=441) claimed to know what personal data is, but 71.5% (n=366) cannot distinguish their difference between sensitive personal data. The improper collection of personal data of minors was observed in 16.5% of the responses obtained and 40.9% of professionals reported making some term of consent available to parents and/or guardians. About the data security mechanisms, 72.1% reported that the service was unprotected, not meeting GDPL standards and with risks of failure and information leakage. It was also observed that 54.8% of dentists use some social network to share images of patients, with WhatsApp being the largest of them (32%). Approximately 68% use access to reports and radiographic images, through the clinic's website (28%), Idoc 49.9% and Cfaz.net (5%). Statistically significant associations ($p < 0.05$) were observed in twelve of the questions asked, when associated with the administrative sphere. **Conclusion:** With the realization of the

study it was possible to observe that most dentists know little about the existence of the GDPR and its applicability within dentistry, that most services lack measures for the protection of data and personal information, in addition to demonstrating the importance of the law for society, especially health-related services.

Keywords: Dentist; Privacy; Computer security; Law enforcement; Confidentiality.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Agência Nacional de Proteção de Dados
AUPD	Autoridade Europeia de Proteção de Dados
CF	Constituição Federal
CFM	Conselho Federal de Medicina
CFO	Conselho Federal de Odontologia
CRB	Colégio Brasileiro de Radiologia e Diagnóstico por Imagem
DICOM	Digital Imaging and Communications in Medicine
LGPD	Lei Geral de Proteção de Dados
PACS	Picture Archiving and Communications Systems
PADI	Programa de Acreditação em Diagnóstico por Imagem
RGPD	Regimento Geral de Proteção de Dados
SBIS	Sociedade Brasileira de Informática em Saúde
UE	União Europeia

SUMÁRIO

1. INTRODUÇÃO	1
2. REVISÃO DA LITERATURA	3
3. OBJETIVOS	11
4. METODOLOGIA	12
5. RESULTADOS	14
6. DISCUSSÃO	22
7. CONCLUSÃO	26
REFERÊNCIAS	27
APÊNDICE	33
ANEXO	36

1. INTRODUÇÃO

O avanço da tecnologia proporcionou uma mudança no contexto da estruturação, armazenamento e compartilhamento de dados entre diversos setores da sociedade, como os dados na área da saúde, por exemplo, o que facilitou a comunicação entre diversos profissionais (Pinochet et al., 2014). Dentro da certificação de um serviço e com o crescente avanço científico e tecnológico que ocorre em todo o mundo, torna-se fundamental, não só por meio de empresas privadas, como também das públicas, regular, de maneira efetiva, o gerenciamento e a proteção dos dados pessoais dos seus usuários, garantindo a privacidade de suas informações (Lima, 2017).

Na literatura científica, o primeiro registro sobre o direito à privacidade surgiu em 1890, em um artigo publicado na Harvard Law Review por Warren e Brandeis, intitulado de *The Right to Privacy* (direito à privacidade), onde os autores descrevem a privacidade como sendo o “direito de ser deixado só” e denunciavam como os meios de comunicação e aparatos tecnológicos invadiam os domínios da vida privada e doméstica, naquela época. Atualmente, a violação e roubo de informações pessoais por meio de ataques virtuais são cada vez mais comuns, chegando a serem comercializadas na *dark web* por altos valores, principalmente informações ligadas à saúde, como mostra o relatório anual da APURA Cyber Intelligence, em 2021.

Mais recentemente, no intuito de aumentar o controle e fornecer uma maior segurança sobre os dados pessoais, a União Europeia (EU), em 2016, criou o Regulamento Geral de Proteção de Dados (RGPD). Esse regulamento baseia-se no princípio de proteção dos direitos fundamentais, como a liberdade e a privacidade e deixa claro que os proprietários dos dados têm total direito sobre suas informações, o que fornece mais controle por parte destes e, consequentemente, maior responsabilidade por parte das empresas (Piurcosky et al., 2019).

Por conseguinte e inspirada no RGPD, surge lei nº 13709/2018, denominada Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, no Brasil (Finkelstein, Finkelstein, 2019; Aragão, Schiocchet 2020).

A LGPD é reflexo da busca internacional pelo direito à privacidade e proteção de dados pessoais, com o intuito de que as pessoas tenham conhecimento e controle sobre a coleta e o gerenciamento de suas informações (Freitas, Silva, 2018). A presente lei estabelece um conjunto de princípios a serem seguidos, como os de finalidade de uso, adequação e limitação ao que é necessário, livre acesso do titular, qualidade e precisão dos dados, transparência, segurança, prevenção, não discriminação, além de responsabilidade e prestação de contas. Com essa regulamentação são esperadas mudanças nos setores tecnológicos, jurídicos e funcionais de diversas instituições e, quando do descumprimento dessas obrigações, estes ficarão sujeitos às penalidades administrativas aplicáveis pela autoridade nacional (BRASIL 2018).

Os dados dos pacientes atendidos em clínicas odontológicas são considerados sensíveis e necessitam de maior proteção, portanto é preciso garantir o controle e a segurança dessas informações, como aquelas relacionadas as patologias do paciente, as receitas médicas, aos exames complementares e, até mesmo, informações financeiras, devendo ser uma preocupação constante de todos os profissionais da área (Aragão, Schiocchet 2020). Sendo assim, os serviços que prestam assistência odontológica no Brasil fazem parte do grupo que deve se adequar à LGPD, para coletar, armazenar, processar e compartilhar dados de maneira segura e confidencial.

Por esta razão e atrelado à carência de estudos que tratem deste assunto literatura, o objetivo desta pesquisa é analisar e compreender a segurança no gerenciamento dos dados pessoais e compreender a realidade de entidades prestadoras de assistência odontológica brasileiras, quanto às adequações à LGPD.

2. REVISÃO DA LITERATURA

2.1 O que são Dados Pessoais

Tratando-se de uma lei de proteção de dados, é importante que as definições traduzam exatamente o que cada ponto significa, afim de assegurar o tipo de regra que a ela se aplica ou não. Sendo assim, deve-se dar atenção as especificações sobre os diferentes tipos de dados, bem como o mecanismo de gerenciamento das informações em cada situação, tendo em vista a ausência de exemplificações na íntegra (Batista, Obergón, 2020; Dourado, Aith, 2022).

Os fundamentos da LGPD estão expressos no artigo 2, que trata, entre outros pontos do respeito à privacidade, assegurando o direito à vida privada; a liberdade de expressão, de informação, de comunicação e de opinião, que são direitos garantidos pela Constituição Federal (CF), bem como o direito da inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor (Brasil, 2018).

Os dados pessoais são informações que podem ser usadas para identificar uma pessoa, seja direta ou indiretamente. De acordo com o artigo 5º da LGPD, nos incisos I e II, dado pessoal é definido como informação relacionada a pessoa natural identificada ou identificável, um artefato que se possa individualizar uma pessoa (nome, endereço, estado civil, idade, etc.), ou seja, é aquela informação específica e capaz de particularizar. Já os dados pessoais sensíveis são informações delicadas e preciosas, como dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018).

Esses dados fazem parte valiosa de informações que geralmente as pessoas compartilham com empresas, serviços, governo e instituições com fins comerciais. Por serem informações importantes, devem estar protegidas e receber tratamento adequado, garantindo o direito à privacidade e direitos fundamentais, principalmente no tocante aos dados sensíveis ligados à saúde (Kroes et al., 2021).

Essa última categoria merece uma maior proteção e cuidado, pois estão relacionados a informações que podem gerar prejuízos, como discriminação e

constrangimentos, podendo trazer consequências à liberdade do seu titular. Dessa forma, o gerenciamento desses dados deve ocorrer somente com o devido consentimento dos seus proprietários, e são sobre esses dados que o presente estudo visa explorar e obter informações relacionadas à odontologia.

2.2 Segurança da Informação

O dado é a base do saber e a peça fundamental para a informação, é de suma importância para a humanidade e vem sendo, ao longo dos avanços tecnológicos, cada vez mais necessário. Mesmo diante de todo esse progresso científico, ainda não é possível permitir a totalidade de sua segurança, da privacidade e da confidencialidade, sendo necessário a adoção de medidas que garantam tal proteção (Flores, Silva, 2020).

Estabelecer um mecanismo de segurança da informação é crucial para empresas, instituições governamentais e demais serviços, no intuito de proteger sua integridade, confidencialidade e disponibilidade de informações valiosas. Dentro dessa perspectiva, tem-se notado a preocupação por parte dos indivíduos, já que o aumento da digitalização resultou em uma quantidade crescente de informações pessoais sendo armazenadas e compartilhadas com auxílio de plataformas digitais (Wehrle et al., 2022).

Com o enorme crescimento e propagação das redes sociais no mundo moderno, tornou-se comum e notório os casos de vazamento de dados, quase sempre de forma maliciosa por parte de *hackers*, mas por vezes de forma não intencional pela falta de instrução do titular. A exemplo de caso que tomou grandes proporções, como o da atriz Carolina Dieckmann, que teve suas fotos íntimas vazadas e acabou gerando uma lei que leva o seu nome e que, atrelada a outras conquistas nessa mesma temática, ainda não foram suficientes para atender as necessidades da segurança pessoal no meio digital (Carneiro, Santos, Elder, 2022).

Para que seja possível melhorar a proteção de informações, alguns autores afirmam que a segurança da informação deve estar alicerçada em três pilares principais, que protejam os dados pessoais de cada indivíduo, sendo eles: a confidencialidade, garantindo o acesso à informação somente por pessoas autorizadas; a integridade, garantindo a fiabilidade da informação para que não haja nenhuma alteração que possa comprometer a integridade dos dados, evitando

prejuízos; e, por fim, a disponibilidade, pilar que garante que a informação esteja disponível quando solicitada (Yee, Zolkipli, 2021).

A implementação de medidas de segurança, como a criptografia, autenticação de usuário, backup regulares, controle de acesso de dados, monitoramento e políticas de segurança são ferramentas fundamentais para proteção de informações sensíveis e confidenciais (Mascarenhas Neto, Araújo 2019).

No que se refere a segurança de dados na LGPD, fica sob a responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão vinculado à Presidência da República, o objetivo de zelar, editar e fiscalizar a aplicação das normas e procedimentos da lei. A este órgão fica, também, o compromisso de edição de normas, a interpretação da lei e outras funções (Neves et al., 2021; Finkelstein, Finkelstein, 2019).

2.3 Proteção de Dados

No Brasil, em ordem cronológica, a garantia da privacidade como direito fundamental foi inicialmente estabelecida pelo artigo 5º, inciso X da Constituição Federal (CF). Em seguida, em 1990, com a chegada do código de defesa do consumidor, pôde-se regular os bancos de dados e cadastros dos consumidores. Já em 2002, o Código Civil, por meio do artigo 21, fundamentou aspectos relacionados a vida privada da pessoa natural assegurando que esta deve ser inviolável. Doze anos depois, criou-se o Marco Civil da Internet que trata sobre a disciplina do uso da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres a serem observados por provedores e usuários dos serviços de internet, como os princípios de proteção da privacidade e proteção de dados pessoais.

Essa tutela de proteção como direito fundamental está diretamente ligada com os princípios da dignidade e intimidade, devendo ser garantida e assegurada por meio de medidas técnicas e organizacionais, que impossibilite o compartilhamento e/ou processamento sem o devido consentimento do titular. O processo do ciclo de vida desses dados inicia-se com o repasse das informações por meio do proprietário e, em seguida, os mesmos ficarão armazenados em bancos até serem processados para fins específicos, podendo ser compartilhados com terceiros, como parceiros comerciais ou fornecedores de serviços, e, por fim,

serem descartados de maneira segura, quando não mais necessários (Flores, Silva, 2018).

Dentro das normas da LGPD são estabelecidos quatro sujeitos responsáveis por determinadas funções. O primeiro é o titular dos dados, a pessoa física que fornece a informação e que pode, a qualquer momento, solicitar do controlador mudanças e até mesmo a exclusão de suas informações. Já o controlador é a pessoa natural ou jurídica que decide sobre o processamento dos dados, devendo indicar um terceiro sujeito, o encarregado, que é responsável pela elaboração de relatórios de impacto à privacidade e comunicação com a ANPD. Por fim, o operador é tido como a pessoa que realiza o tratamento de dados pessoais a pedido do controlador (Gregori, 2020).

2.4 Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD) foi aprovado em 2016 e é aplicável desde 2018, revogando a antiga portaria 95/46/CE, e tem o objetivo de proteger os dados pessoais dos cidadãos europeus, garantindo os direitos e liberdades fundamentais, sendo aplicável por todas as instituições e órgãos da União. Os dados pessoais coletados deverão estar justificados e com destino específico, processados de forma legítima, digna e transparente, sob consentimento do seu proprietário e garantindo a segurança adequada (União Europeia, 2016; Lopes, 2020).

O RGPD se aplica a todas as empresas e organizações que trabalham com dados pessoais da União Europeia (EU), independentemente de onde essas empresas estejam localizadas, ou seja, mesmo se as empresas estiverem fora da EU, precisam seguir o RGPD se coletarem algum tipo de dado de algum cidadão europeu. O não cumprimento dessas obrigações poderá implicar em sanções que incluem multas de até 4% do faturamento global anual da empresa, chegando até €20.000.000 para descumprimento de infrações graves (Nahai, 2019; União Europeia, 2016).

O regulamento também aborda o processamento de categorias especiais de dados pessoais ou dados sensíveis, que merecem proteção específica, exigindo que as empresas adotem medidas de segurança adequadas para proteger essas

informações e garantir que estas não sejam roubadas, perdidas ou danificadas (União Europeia, 2016).

Durante o fornecimento dos dados, o titular deverá ser informado sobre os diversos processos pelos quais os mesmos passarão, como a identificação e contato do controlador de suas informações, os fins de tratamento a que se destinam, o tempo pelo qual seus dados serão armazenados, o direito de alteração, exclusão e retirada do consentimento a qualquer momento, bem como o direito de apresentar reclamação à Autoridade Europeia para a Proteção de Dados (AUPD). Esta última é o órgão multinacional responsável pelo controle e aplicação das disposições do RGPD às operações de tratamento realizadas pelas instituições e pelos órgãos da União (União Europeia, 2016).

No tocante ao tratamento de dados pessoais de crianças e adolescentes, a lei europeia diverge da brasileira por aceitar o consentimento do menor, contato que ele tenha mais de 16 anos. Outro ponto importante é referente a segurança e violação dos dados, onde ambas exigem dos controladores e operadores a implementação de programas de governança e privacidade, que garantam a devida proteção dos dados (Iramina, 2020).

2.5 Lei Geral de Proteção de Dados

Inspirada no RGPD, a Lei Geral de Proteção de Dados (LGPD), tida como um avanço do Marco Civil da Internet, trata sobre a obtenção, armazenamento e processamento de dados pessoais no Brasil, seja por meio físico ou digital. A lei tem por objetivo permitir que os titulares tenham total conhecimento e controle sobre suas informações, evitando o compartilhamento ou uso indevido das mesmas. Essa lei somente não se aplica ao tratamento de dados pessoais com fins não econômicos, jornalísticos, acadêmicos, com interesse à segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Sendo assim, o RGPD e a LGPD compartilham muitos pontos em comum (BRASIL, 2018).

Com a finalidade de assegurar a correta execução e lisura da lei e em consonância com o RGPD, o titular deverá, através de um consentimento explícito, demonstrar o desejo de prover suas informações, ficando este ciente de que o presente consentimento poderá ser revogado em qualquer tempo por interesse do

mesmo. Em conjuntura, o sistema de acesso a todo o gerenciamento de suas informações deve ser facilitado, podendo este acessá-las quando necessário (Iramina, 2020).

Os direitos e deveres, bem como a proteção das crianças e adolescentes vem sendo garantidos há muitos anos com a criação de diversas leis voltadas para esse público. No que se refere à LGPD, os menores de idade somente poderão ter seus dados tratados com o consentimento explícito dos pais ou responsável legal, salvo quando a obtenção desses dados seja por necessidade de contatar algum dos responsáveis pela criança ou adolescente, sendo proibido o repasse à terceiros e/ou armazenamento (BRASIL, 2018, BRASIL, 2020).

Sobre o término do tratamento dos dados, também conhecido como o direito ao esquecimento, fica estabelecido que os serviços devem apagar as informações quando estas já não forem mais necessárias para o desempenho de suas atividades, ou quando o titular solicitar a exclusão. O ciclo da vida dessas informações termina quando estas alcançam o tempo estabelecido para o tratamento e também após determinação da ANPD, se violada a lei. Somente em algumas exceções, como para fins de estudos por órgãos de pesquisas, esses dados poderão ser conservados, garantindo a sua anonimização (BRASIL, 2018, Miragem, 2019).

Os descumprimentos das exigências estabelecidas pela lei vão desde advertências, com prazo estipulado para a adoção de medidas corretivas, podendo incluir multas, sanções administrativas, proibição de atividades e, em casos graves, ações criminais. As multas podem variar de acordo com severidade da infração, mas limitadas até 2% do faturamento do serviço e ao valor de R\$ 50.000.000,00.

2.6 Gerenciamento de Dados em Odontologia

Dentro do sistema da saúde, como na odontologia, costumamos armazenar e gerenciar dados pessoais de pacientes, colaboradores e funcionários. Esses dados se encontram, principalmente, em prontuários, sejam eles físicos ou digitais, devendo estar protegidos por conter informações muito íntimas. Para isso, é necessário criar níveis de acesso aos mesmos, nomeando responsáveis para garantir a privacidade de todos, como também a adoção à softwares seguros e eficientes (Costa, 2021).

Nos últimos anos houve uma mudança significativa na forma de obter e armazenar os dados pessoais nos prontuários odontológicos, com o desenvolvimento de prontuários padronizados, capazes de armazenar diversas informações clínicas e administrativas de grande valia para os usuários. De certa forma, fortalece o sistema de proteção e facilita a comunicação entre as diversas categorias da saúde, mas não protege de interferências indevidas, permitindo que o compartilhamento sem a autorização prévia do titular possa acontecer de forma rápida e frequente (Holanda, Mello e Zimmermann, 2010).

As informações armazenadas dentro desses prontuários fazem parte de um arsenal de dados íntimos, como por exemplo os exames de imagens, usados com a finalidade diagnóstica para diversas patologias e que podem revelar informações importantes de cada paciente. Com a obtenção de imagens radiográficas digitais, pôde-se ter acesso ao exame com uma melhor qualidade e em curto espaço de tempo, já que esta dispensa o processo de revelação convencional e utiliza softwares para corrigir algumas falhas (Bruniere, Tanaka e Ito, 2011).

Com o objetivo de fornecer um padrão para o processamento, armazenamento e compartilhamento de dados referentes a exames de imagens, o padrão DICOM (Digital Imaging and Communications in Medicine) se tornou a principal ferramenta de comunicação. Esse padrão constitui um mecanismo eficiente de integração, comunicação e troca de dados entre profissionais da saúde, por meio de dispositivos eletrônicos (Herrmann, et al., 2021).

O padrão DICOM é uma das principais ferramentas de troca de imagens da área da saúde, incluindo diversas especialidades odontológicas e agrupa não só a imagem radiográfica. Com a utilização do DICOM, pretende-se que as imagens sigam o mesmo formato e sejam capazes de serem lidas por diversos programas de radiografias, preservando também sua estrutura de dados e valor legal. Geralmente esse padrão funciona por meio de sistemas baseados em PACS (Picture Archiving and Communications Systems) ou sistema de comunicação de arquivamento de imagem, que atua para integrar a aquisição, armazenamento, recuperação e visualização de imagens (Burgess, 2015).

No que diz respeito à proteção dos dados radiográficos, a norma do Programa de Acreditação em Diagnóstico por Imagem (PADI), pertencente ao Colégio Brasileiro de Radiologia e Diagnóstico por Imagem (CBR), diz que o serviço de radiologia deve garantir que os dados do sistema de informação estejam dentro

dos requisitos de segurança pré-estabelecidos, na confidencialidade e confiabilidade dos dados relacionados ao paciente, além de assegurar que as informações compartilhadas na internet estejam protegidas por algum mecanismo de segurança atualizado. Dentro dessa nova realidade e sabendo que os exames de imagens e prontuários odontológicos armazenam dados sensíveis, é notório que os serviços de odontologia deverão sofrer mudanças e se adequarem às exigências da LGPD.

3. OBJETIVOS

2.1 Objetivo Geral

- Descrever e compreender a realidade dos serviços que prestam assistência odontológica do Brasil, quanto às adequações à Lei Geral de Proteção de Dados Pessoais (LGPD).

2.2 Objetivos Específicos

- Verificar a realidade de unidades prestadoras de assistência odontológica (clínicas), consultórios privados e públicos em relação ao gerenciamento de dados pessoais sensíveis dos seus usuários;
- Compreender o conhecimento dos cirurgiões-dentistas quanto a proteção de dados pessoais;
- Identificar se as entidades possuem certificação de acreditação em diagnóstico por imagem em odontologia;
- Delinear o sistema de comunicação de imagens clínico/radiográficas entre profissionais.

4. METODOLOGIA

O presente estudo é de caráter descritivo e transversal, com abordagem quantitativa e qualitativa dos dados. O mesmo foi registrado na Plataforma Brasil e aprovado pelo Comitê de Ética em Pesquisa da Universidade Federal da Paraíba (CEP-UFPB), sob parecer CAAE: 60717822.4.0000.5188, respeitando assim a resolução 466/12 do Conselho Nacional de Saúde/ Ministério da Saúde. Todos os indivíduos que participarem do estudo foram convidados a cooperar e concordem com o Termo de Consentimento Livre Esclarecido (TCLE) e esclarecidos dos objetivos da pesquisa (ANEXO I).

O cálculo amostral foi realizado através da ferramenta online OpenEpi, considerando o tamanho da população de 362.303 cirurgiões-dentistas inscritos no Conselho Federal de Odontologia (CFO) (<http://website.cfo.org.br/estatisticas/quantidade-geral-de-entidades-e-profissionais-ativos/> Acessado em 2021). Considerou-se que 50% (frequência antecipada) dos participantes estariam a par das recomendações do CFO. Foi estabelecido um intervalo de confiança de 95% e o efeito de desenho (deff) de 2.0. A partir desses parâmetros, foi definido um tamanho amostral de 374 dentistas distribuídos por todo o Brasil.

A amostra do estudo foi do tipo não probabilística e aleatória, baseada na disponibilidade dos cirurgiões-dentistas em responder ao questionário disponibilizado previamente por meio da plataforma *Google Forms*. A primeira sessão do questionário se referia ao TCLE, que garantia a confidencialidade dos dados e informava aos participantes os objetivos do estudo e a sua participação voluntária. O consentimento dos dentistas para participação do estudo ficou estabelecido quando eles clicaram no botão "Li e estou de acordo com o termo do estudo" para responder a pesquisa.

O questionário foi divulgado pelos pesquisadores em grupos de *Whatsapp*®, *Instagram*®, *Facebook*®, *Telegram*® e via e-mail, entre os meses de setembro de 2022 até janeiro de 2023, sendo solicitado que os participantes realizassem o encaminhamento do mesmo para outros cirurgiões-dentistas (amostra por *snowball sampling*), fazendo com que ocorresse o alcance do mesmo em todo território nacional.

Após obtidos, os dados foram exportados e tabulados em uma planilha de Excel, para análise no softwares IBM SPSS® (25.0, IBM Corporation, Armonk, New York, EUA). Os dados foram submetidos inicialmente a uma análise descritiva e exploratória para determinação das frequências absolutas e relativas. Em seguida, associações estatisticamente significantes foram avaliadas por meio do teste qui-quadrado, com intervalo de confiança de 95%.

5. RESULTADOS

Após a leitura e aceitação do termo, 512 profissionais responderam devidamente o questionário em diversas cidades do país. Em relação à esfera administrativa, observou-se que 323 cirurgiões-dentistas (63,1%) atuavam apenas no serviço privado e somente 99 (19,3%) eram profissionais vinculados apenas na esfera pública, enquanto que 90 (17,6%) atuavam em ambas as esferas. Entre todos os profissionais, 64,3% afirmaram fotografar seus pacientes durante a consulta odontológica, mas apenas 35,2% faziam uso dessas imagens através de mídias sociais, como evidencia a tabela 1.

Os participantes foram questionados quanto ao seu conhecimento a respeito do que seria dados pessoais e sobre a implementação da Lei Geral de Proteção de Dados (LGPD) – lei nº 13. 709/2018, no Brasil. A grande maioria 86,1% (n=441) afirmou saber o que são dados pessoais, mas cerca de 71,5% declararam não saber distinguir a diferença entre dados pessoais e dados pessoais sensíveis. Já sobre o conhecimento sobre a lei, 59,8% não possuía qualquer informação sobre a mesma e somente 41,4% estavam cientes de que ela estava em vigor desde 2020.

Perguntados sobre a coleta e gerenciamento de dados pessoais, foi possível observar que 65,8% dos odontólogos afirmaram não recolher dados pessoais sensíveis dos pacientes nos estabelecimentos onde prestam serviços. Para analisar o conhecimento sobre a definição desses dados foi deixado uma caixa para respostas subjetivas e as que mais prevalentes foram: dados documentais, dados mais sigilosos, informações étnicas, dados genéticos e médicos. Já sobre a obtenção de dados pessoais de crianças e adolescentes, 40,2% da amostra afirmou que realizava tal coleta e que utilizava algum termo de consentimento com os responsáveis, 42,4% afirmou não coletar dados pessoais desse público, e apenas 17,4% realizava tal conduta de maneira inadequada, sem a utilização de algum termo.

Para a grande maioria dos entrevistados (73%), os dados dos colaboradores e clientes/pacientes estão dispostos de forma organizada, atendendo os requisitos da LGPD. Entretanto, 56,6% não sabem ou afirmam que esses mesmos dados não estão devidamente justificados, com finalidade de uso específica.

Quando se refere ao manuseio, compartilhamento e tratamento dos dados pessoais, os indivíduos foram questionados sobre a existência de algum tipo de

consentimento para a utilização destes, no momento da solicitação de envio desses dados. 37,3% afirmaram que havia algum termo solicitando ao titular a permissão para compartilhamento desse conteúdo. Em contrapartida, 62,7% alegaram que não sabiam informar ou declararam não solicitar qualquer consentimento prévio ao compartilhamento dessas informações. Caso o dono quisesse saber como os seus dados estariam sendo tratados, 80,9% dos profissionais afirmaram que poderiam atendê-lo, mas somente 51% dos serviços parecem possuir documentações e práticas relacionadas à gestão da privacidade da informação.

Foi possível verificar, também, que cerca de 77% dos profissionais utilizam o meio digital para receber ou processar os exames de imagem. Atrelado a isso, 68% informaram ter acesso a serviços de laudos e imagens radiográficas, entre os quais pode-se citar: recebimento de imagens via iDoc (49,8%), site da clínica (26,4%), Cfaz.net (5,5%), além de outros meios (39,6%). Notou-se que 51,6% dos dentistas costumam usar alguma rede social para compartilhamento de imagens de pacientes, sendo o WhatsApp a mais popular delas (31,1%). As distribuições de todas as respostas às variáveis relacionadas aos profissionais e às adequações dos serviços de assistência odontológica referentes à LGPD estão listadas abaixo.

Tabela 1. Distribuição das frequências relativas (N) e percentuais (%) às respostas dadas a cada uma das categorias das variáveis relacionadas aos profissionais e às adequações dos serviços de assistência odontológica referentes à LGPD (n=512).

Variável	Categorias	n	%
Esfera administrativa onde trabalha	Pública	99	19,3
	Privada	323	63,1
	Pública/Privada	90	17,6
Você fotografa seus pacientes?	Sim	329	64,3
	Não	183	35,7
Você usa imagens de pacientes em mídias sociais?	Sim	180	35,2
	Não	332	64,8
Você sabe o que são dados pessoais?	Sim	441	86,1
	Não	71	13,9
Você conhece a nova Lei Geral de proteção de dados (LGPD) – lei nº 13.709/2018?	Sim	206	40,2
	Não	306	59,8

Você sabia que a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em agosto de 2020?	Sim	212	41,4
	Não	300	58,6
Você sabe a diferença entre dados pessoais e dados pessoais sensíveis?	Sim	146	28,5
	Não	366	71,5
Você coleta dados pessoais sensíveis?	Sim	175	34,2
	Não	337	65,8
Você realiza o tratamento de dados pessoais de crianças e adolescentes?	Sim, mas não uso termo de consentimento dos pais e/ou responsáveis	89	17,4
	Sim, e uso o termo de consentimento dos pais e/ou responsáveis	206	40,2
	Não	217	42,4
O serviço possui dados pessoais, de seus colaboradores e clientes, de forma organizada?	Sim	374	73
	Não	138	26
Os tratamentos de dados realizados estão devidamente justificados?	Sim	222	43,4
	Não	55	10,7
	Não tenho conhecimento	235	45,9
Há a coleta e registro de algum tipo de consentimento para utilização dos dados pessoais cadastrais no momento da solicitação de envio desses dados?	Sim	191	37,3
	Não	136	26,6
	Não tenho conhecimento	185	36,1
O titular é informado sobre o que será feito com os seus dados pessoais coletados?	Sim	314	61,9
	Não	195	38,1
	Sim	414	80,9

Caso o paciente queira saber como seus dados pessoais são tratados, haveria alguma forma de atendê-lo?	Não	98	19,1
O serviço possui documentações e práticas relacionadas à gestão da privacidade da informação?	Sim	261	51
	Não	251	49
As operações de tratamento de dados pessoais estão protegidas?	Sim	275	53,7
	Não	237	46,3
Existe algum mecanismo de gestão para prevenir ou minimizar falhas de segurança, como o vazamento de dados?	Sim	147	28,7
	Não	365	71,3
Os dados pessoais coletados são compartilhados com terceiros?	Sim	61	11,9
	Não	451	88,1
Você utiliza alguma rede social para compartilhamento de exames de imagens de seus pacientes?	Não	248	48,4
	Whatsapp	159	31,1
	Facebook	19	3,7
	Instagram	86	16,8
	E-mail	128	25
	Outro	23	4,5
O serviço está preparado para atender à solicitação dos titulares de dados, como exclusão, compartilhamento, armazenamento e outros direitos relacionados as operações de tratamento dos seus dados pessoais?	Sim	274	53,5
	Não	238	46,5
O serviço possui alguma certificação de acreditação em diagnóstico por imagem?	Sim	68	13,3
	Não	444	86,7
Você utiliza algum serviço de acesso à laudos e imagens radiográficas?	Sim	347	67,8
	Não	165	32,2
O serviço utiliza o padrão DICOM para compartilhamento de exames de imagem?	Sim	259	50,6
	Não	253	49,4

Você recebe radiografias pela internet?	Site da clínica	135	26,4
	Idoc	255	49,8
	Cfaz.net	28	5,5
	Outro	203	39,6
Como você visualiza os exames de imagem?	Filme impresso	286	55,9
	Digital	396	77,3

Os resultados do teste qui-quadrado são apresentados a seguir, juntamente com a análise post-hoc para as respostas específicas do questionário que apresentaram associação estatisticamente significativas. Adotou-se como critério de significância as associações cujos valores de p foram menores do que 0,05 e os resíduos ajustados padronizados maiores que 1,96 e menores que -1,96.

Observou-se que houve efeito estatisticamente significativo entre a esfera administrativa e a atitude de fotografar os pacientes durante a consulta ($p=0,000$), bem como para o uso dessas imagens em mídias sociais ($p=0,0001$). Também foi possível identificar significância relevante entre a esfera administrativa e o conhecimento do profissional quanto a diferença entre dados pessoais e dados pessoais sensíveis ($p=0,045$). As demais associações observadas para variáveis dicotômicas estão detalhadas na tabela 2.

Tabela 2. Análise post-hoc das variáveis dicotômicas relacionadas a avaliação do grau de conformidade à LGPD.

Questão	Esfera administrativa	Resíduos ajustados		p valor
		Sim	Não	
Você fotografa seus pacientes?	Público	3,9	-3,9	$p=0,000$
	Privado	-7,4	7,4	
	Público/privado	2,7	-2,7	
Você usa imagens de pacientes em mídias sociais?	Público	1,0	-1,0	$p=0,001$
	Privado	-3,5	3,5	
	Público/privado	2,3	-2,3	
Você sabe a diferença entre dados pessoais e dados pessoais sensíveis?	Público	1,4	-1,4	$p=0,045$
	Privado	,7	-,7	
	Público/privado	2,5	-2,5	
O serviço possui dados pessoais de seus colaboradores e clientes de forma organizada?	Público	3,1	-3,1	$p=0,002$
	Privado	-,6	,6	
	Público/privado	-3,3	3,3	

As operações de tratamento de dados pessoais estão protegidas?	Público	1,4	-1,4	p=0,045
	Privado	,7	-,7	
	Público/privado	-2,5	2,5	
O serviço está preparado para atender à solicitação dos titulares de dados, como exclusão, compartilhamento, armazenamento e outros direitos relacionados as operações de tratamento dos seus dados pessoais?	Público	2,4	-2,4	p=0,036
	Privado	-2,2	2,2	
	Público/privado	-,7	,7	
Você utiliza algum serviço de acesso à laudos e imagens radiográficas?	Público	5,7	-5,7	p=0,000
	Privado	-9,1	9,1	
	Público/privado	2,2	-2,2	
O serviço utiliza o padrão DICOM para compartilhamento de exames de imagem?	Público	5,4	-5,4	p=0,000
	Privado	-7,4	7,4	
	Público/privado	,8	-,8	

Evidenciou-se, também, diferença estatística entre o setor administrativo e a relação do conhecimento do profissional sobre a coleta de algum consentimento para a utilização de dados pessoais cadastrais, em algum momento em que esses dados fossem tratados ($p=0,041$). No entanto, na análise post-hoc dos resultados, essa associação esteve presente, principalmente, na esfera pública, estando relacionada à falta de conhecimento ou não realização da ação mencionada na pergunta, conforme expressa a tabela 3.

Tabela 3. Análise post-hoc da relação entre a esfera administrativa e a coleta de consentimento para tratamento de dados pessoais, no momento da solicitação de envio dos mesmos.

Questão	Esfera administrativa	Resíduos ajustados			p valor
		Sim	Não	Não tenho conhecimento	
Há a coleta e registro de algum tipo de consentimento para utilização dos dados pessoais cadastrais no	Público	,3	2,1	-2,2	p=0,041
	Privado	-1,6	-,8	2,4	
	Público/privado	1,3	-1,8	,4	

momento da solicitação de
envio desses dados?

Os fatores relacionados ao compartilhamento de imagens de pacientes em redes sociais, de igual modo, apresentaram significância ($p=0,000$). Entretanto, após a análise post-hoc observou-se que, das redes sociais listadas, o Whatsapp e o Instagram foram as mais utilizadas pelos profissionais para esse tipo de função. Esses e os valores das demais redes podem ser visualizados na tabela 4.

Tabela 4. Análise post-hoc da relação entre a esfera administrativa e o uso de rede sociais para compartilhamento de exames de imagens.

Esfera administrativa	Resíduos ajustados							p valor $p=0,000$
	Não	Whatsapp	Facebook	Instagram	E-mail	Duas ou mais	Outro	
Público	-2,7	3,3	1,3	-2,0	,8	,6	2,3	
Privado	5,2	-2,5	-,9	-,5	-1,9	-2,1	-1,5	
Público/ privado	-2,0	-1,5	-,8	3,0	,9	1,4	-1,4	

Para o recebimento de exames de imagem pela internet, o Idoc e outras plataformas não especificadas foram as mais utilizadas, apresentando efeito estatisticamente provável ($p=0,000$). A análise após ajustes dos resíduos se encontra na tabela 5.

Tabela 5. Análise da relação entre a esfera administrativa e o recebimento de exames de imagens pela internet.

Esfera administrativa	Resíduos ajustados					p valor $p=0,000$
	Site da clínica	IDoc	Cfaz.net	Duas ou mais	Outra	
Público	,7	3,8	1,9	3,2	-6,3	
Privado	-,1	-5,0	-1,2	-4,1	8,8	
Público/ privado	1,0	,4	-1,1	,2	-1,1	

A relação entre a esfera administrativa e a forma de visualização dos exames de imagens foram analisadas juntas e isoladamente. Com isso, foi possível verificar significância entre os fatores ($p=0,000$), como mostra a tabela 6.

Tabela 6. Análise post-hoc da relação entre a esfera administrativa e a modalidade de visualização de exames de imagem.

Esfera administrativa	Resíduos ajustados			p valor
	Filme impresso	Digital	Filme impresso e digital	
Público	-6,4	4,7	,7	p=0,000
Privado	9,8	-4,0	-4,5	
Público/ privado	-2,0	-1,8	3,7	

6. DISCUSSÃO

A falta de conhecimento sobre um assunto tão pertinente e delicado, como a proteção de dados pessoais de pacientes, pode ser motivo de grandes problemas, principalmente após entrar em vigor uma lei que garanta direitos de proteção de imagens, dados e informações pessoais, muitas das quais são sensíveis e de caráter sigiloso. A obtenção dos dados deste estudo pôde revelar a falta de conhecimento por parte dos profissionais, a baixa popularidade da lei no setor odontológico e um grande número de cirurgiões-dentistas vinculados à esfera administrativa privada, em desconformidade com a Lei Geral de Proteção de Dados.

As informações pessoais, como fotos e/ou vídeos de pacientes, exames complementares e prontuários odontológicos são considerados dados sensíveis e devem estar bem protegidos, mas isso nem sempre é possível. Estudos evidenciam que muitos profissionais armazenam ou compartilham dados de terceiros sem a devida autorização, bem como desconhecem a legislação que trata sobre o uso de imagens (Leal et al., 2018; Nascimento, 2016). Esses estudos corroboram com os achados na presente pesquisa, demonstrando o alto índice de profissionais que fotografam seus pacientes durante o atendimento e os que afirmam fazer uso de mídias sociais para compartilhamento de tais dados.

O fato de usar imagens do paciente em mídias sociais ficou ainda mais comum após a resolução 196/2019 do CFO autorizar a divulgação de autoretratos (selfie) e de imagens relativas ao diagnóstico e ao resultado final de tratamentos odontológicos. Sabe-se que a divulgação dessas imagens tem interesse comercial e, portanto, elas costumam ser divulgadas em serviços privados, e que alguns profissionais fazem uso de forma indiscriminada. Esse fato fica ainda mais evidente, no presente estudo, após a análise estatística evidenciar significâncias embutidas nas esferas administrativas privada e público/privada.

No tocante ao compartilhamento de dados com terceiros, o serviço fica inteiramente proibido se, por acaso, não houver autorização prévia por meio do titular. Alguns estudos mostram que essa autorização prévia, principalmente para divulgação de imagens e/ou vídeos de pacientes, se dá, quando existe, de forma verbal e não por escrita (Nascimento, 2016; Leal, et al., 2018). Na análise desta pesquisa foi observada uma divergência no quesito compartilhamento de imagens

com terceiros, onde, inicialmente, 348 profissionais (88,3%) afirmaram não distribuir esses dados com outras pessoas, mas 211 (53,5%) relataram usar alguma rede social para o compartilhamento do mesmo material, principalmente por redes sociais popularizadas como Whatsapp e Instagram. Esse achado divergente entre as perguntas pode estar ligado ao receio do profissional em assumir realizar tal conduta.

O fato da LGPD ter sido criada apenas em 2018 e implementada em 2020, é notório que a sua popularização seja baixa após apenas três anos de vigência, tendo em vista que esse processo de difusão não é formalizado e institucionalizado, o que repercute no pouco conhecimento dos profissionais, tanto no que diz respeito à existência como entendimento da lei. O baixo nível de conhecimento sobre esse tema pelos cirurgiões-dentistas demonstra a importância dos órgãos fiscalizadores e que regem a odontologia no país, em dar visibilidade e notoriedade a legislação vigente que trata sobre o assunto.

O tratamento de dados pessoais sensíveis, de acordo com a LGPD, deverá ocorrer quando o titular ou responsável legal consentir, salvo para situações específicas, como procedimentos realizados por profissionais da saúde e autoridade sanitária. Dessa forma, o conhecimento sobre esse conjunto de dados é de extrema importância por parte dos profissionais, a fim de evitar o gerenciamento incorreto dos mesmos (Gregori, 2020). Nesta pesquisa, o fato dos entrevistados não saberem distinguir dados pessoais de dados pessoais sensíveis e afirmarem não coletar esse tipo de informação dos pacientes pode estar associado com a falta de conhecimento e favorecer tomadas de decisões incorretas no processo de gerenciamento dos dados.

Sobre a obtenção e tratamento de dados pessoais de crianças e adolescentes, conforme o art. 14 da vigente lei, deverá pelo menos um dos pais ou responsável legal dar o consentimento para uso de tais, salvo em poucas exceções. Neste período, o menor é visto como um ser em construção e precisa ter seus direitos garantidos e mantidos pela sociedade, Estado e família, de maneira especial (Costa Motta, Sarlet Sales, 2021). Apesar de pequena, ainda houve uma parcela (16,5%) que afirmou fazer uso desses dados sem o consentimento claro por parte dos pais e/ou responsável legal, o que viola as conquistas alcançadas até aqui. Estudos evidenciam que os cirurgiões-dentistas conhecem e jogam importante o uso do termo de consentimento prévio em consultas com crianças e

adolescentes, mas que na prática isso nem sempre acontece (Garbin et al., 2007, Sales-Peres et al., 2011, Yarid et al., 2012).

Os prontuários são fontes de inúmeras informações do paciente e devem ser mantidos em segurança, seja ele físico ou digital. O tratamento desses dados em meio virtual, geralmente se dá através de softwares que, segundo a Sociedade de Informática em Saúde (SBIS), deve atender o Nível de Garantia de Segurança 1 e 2 (NGS1 e NGS2), pois ambos desempenham funções importantes como controle de acesso e autenticação, disponibilidade, comunicação remota, auditoria e exigência de utilização de certificados digitais para processos de assinatura e autenticação (Muniz, Hessel, 2019).

Esses softwares nem sempre estão disponíveis ou não há mecanismo de gestão para prevenir ou minimizar falhas de segurança, conforme observado nesta pesquisa. Corroborando com este achado, Barbalho et al. (2017) atestaram que o sistema e-SUS AB PEC não implementa todos os requisitos obrigatórios para certificação de segurança e que, inclusive, o sistema seria reprovado caso fosse submetido a um processo de certificação da SBIS, em conjunto com o Conselho Federal de Medicina (SBIS/CFM).

De acordo com Novaes et al. (2019), o serviço de saúde deve apresentar documentações e práticas relacionadas à gestão da privacidade das informações. Para isso, é necessário que este objeto seja claro e de fácil interpretação, apresentando de forma simplificada as instruções referentes ao processo de tratamento dos dados pessoais do indivíduo. Os autores ainda destacam que somente esse documento não seria suficiente como política de privacidade e reiteram a importância de detalhar ao titular os dados coletados e sua finalidade de base legal. Neste aspecto, foi observado que boa parte dos profissionais questionados (51%) relatou a existência de algum tipo de documentação e/ou práticas relacionadas a este assunto, bem como a facilidade de acesso dos proprietários, caso necessário.

O recebimento, armazenamento e compartilhamento de imagens radiográficas é outro ponto importante, tendo em vista os avanços atuais e a facilidade de obtenção dessa ferramenta pelo meio digital. Observamos que 67,8% da amostra deste estudo recebe esse tipo de exame através da internet, seja pelas plataformas Idoc, Cfaz.net, pelo próprio site da clínica e/ou a partir de outro meio. Mesmo diante desse grande percentual de exames digitais, ainda se observa um

número considerado de profissionais que recebem e armazenam a radiografia em filme impresso, dado que requer maior cuidado no tocante ao seu processamento.

O objetivo do Programa de Acreditação em Diagnóstico por Imagem (PADI) é a busca pela excelência nos serviços de diagnóstico por imagem, permitindo que os dados compartilhados na internet estejam protegidos por *firewall* ou outro mecanismo de proteção, assegurando a privacidade dos mesmos. Infelizmente este serviço é um pouco distante da realidade encontrada no cenário atual, pois, durante o período de aplicação do objeto de estudo desta pesquisa, apenas 1 (0,19%) profissional mencionou o PADI como serviço de certificação de acreditação em diagnóstico por imagem em seu local de trabalho.

Por fim, algumas limitações puderam ser identificadas, como a carência de estudos similares na literatura, tanto em nível nacional, como internacional, demonstrando o ineditismo da presente pesquisa, mas dificultando a comparação do cumprimento da legislação em diferentes partes do país e também fora dele. Outra limitação diz respeito ao receio profissional em responder algumas perguntas que estejam associadas à sua falta de conhecimento e à prática indevida de ações sobre o determinado assunto, como foi comprovado com as divergências das respostas em questões específicas.

7. CONCLUSÃO

A presente pesquisa observou a grande desconformidade e desconhecimento entre os cirurgiões-dentistas em relação às adequações necessárias à Lei Geral de Proteção de Dados, além de destacar que a maioria dos serviços carece de medidas para proteção de dados e informações pessoais, demonstrando a importância da lei para a sociedade, principalmente a serviços ligados à saúde. Sendo assim, este estudo pôde fornecer informações necessárias sobre o atual cenário do gerenciamento de dados pessoais em odontologia no Brasil, servindo de subsídios para os órgãos regulatórios em território nacional se embasarem e atuarem na disseminação da lei e implementação de práticas de gestão de segurança, fazendo com que os serviços se adequem à mesma.

8. REFERÊNCIAS

Pinochet LHC, Lopes AS, Silva JS. Inovações e tendências aplicadas nas tecnologias de informação e comunicação na gestão da saúde, Revista de Gestão em Sistema de Saúde. 2014;3(2) 11-29, doi: 10.5585/rgss.v3i2.88.

Lima MI. Do direito à proteção de dados em matéria de saúde na sociedade de informação. Arquivo Jurídico. 2017;4(1) 1 – 24, ISSN 2317-918X.

APURA CYBER INTELLIGENCE, 2021 O ano em resumo. p. 1 - 29, 2021.

Warren SD, Brandei LD. Right to privacy. Harvard Law Review, 1890;4(5) 193-220.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: General Regulation Data Protection (Regulamento Geral sobre Proteção de Dados). Bruxelas, 27 abr. 2016. Disponível em: <eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acessado em 12 nov. 2021.

Piurcosky PF, Costa MA, Frogeri RF, Calegario LL. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. Suma de negócios. 2019;10(23) 89-99, doi: 10.14349/sumneg/2019.V10.N23.A2.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 12 nov de 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74 jan. 2002. Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=10406&ano=2002&ato=ac5gXVE5ENNpWT07a>. Acesso em: 28 nov. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 12 nov de 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 nov. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a lei geral de proteção de dados pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2021.

BRASIL. GOVERNO DIGITAL. Guia de Proteção de Dados Pessoais – Crianças e Adolescentes. Fundação Getúlio Vargas, versão 1.0, 2020; 1-35. Acesso em: 29 nov. 2022.

Miragem B. Lei geral de proteção de dados (Lei 13.709/2018) e o direito do consumidor. *Revista dos Tribunais*, 2019;1009(1), 1-35.

Finkelstein ME, Finkelstein C. Privacidade e lei geral de proteção de dados pessoais. *Revista de Direito Brasileira*. 2019;23(9) 284-301.

Aragão SM, Schiocchet T. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *Rev Eletron Comun Inf Inov Saúde*. 2020;14(3) 692-708, doi: <https://doi.org/10.29397/reciis.v14i3.2012>.

Freitas MC, Silva MM. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*. 2018;3(4) 1-7, ISSN: 2468-4376.

COLÉGIO BRASILEIRO DE RADIOLOGIA E DIAGNÓSTICO POR IMAGEM-CBR. Norma do Programa de acreditação em diagnóstico por imagem-Padi; versão 4.0, 2020.

Herrmann MD, Clunie DA, Fedorov A, Doyle SW, Pieper S, Klepeis V, et al. Implementing the DICOM standard for digital pathology. *Journal of Pathology Informatics*. 2021;1(37) 1-18, doi: 10.4103/jpi.jpi_42_18.

Batista LS, Obregón MFQ. Os impactos do Regulamento Europeu Geral sobre Proteção de Dados (EU GDPR) no Brasil. *Derecho y Cambio Social*, 2020;6(1)1-15, ISSN: 2224-4131.

Kroes SK, Janssen MP, Groenwold RH, Leeuwen MV. Evaluating privacy of individuals in medical data, *Health Informatics J* . 2021 Apr-Jun;27(2):1460458220983398. doi: 10.1177/1460458220983398.

Dourado DA, Aith FMA. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais, *Revista de Saúde Pública*, 2022;56(80)1-7, doi:10.11606/s1518-8787.2022056004461.

Flores MR, Silva RL. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. *Revista de Direito*. 2020;12(2) 1-34, doi: 10.32361/2020120210327.

Wehrle K, Tozzi V, Braune S, Roßnagel F, Dikow D, Paddock S, et al. Implementation of a data control framework to ensure confidentiality, integrity, and availability of high-quality real-world data (RWD) in the NeuroTransData (NTD) registry. *JAMIA*. 2022 Mar 9;5(1):ooac017. doi: 10.1093/jamiaopen/ooac017. eCollection 2022 Apr.

Carneiro LVV, Santos JN, Elder GOB. Diereito cibernético: o impacto gerado pela lei Carolina Dieckmann no combate aos crimes virtuais realizados contra as

crianças e adolescentes. Rev Ibero-Americana de Hum, Ciên e Edu - REASE, 2022;8(11)2061-2080, doi: 10.51891/rease.v8i11.7793.

Yee CK, Zolkipli MF. Review on Confidentiality, Integrity and Availability in Information Security, Journal of ICT in Education. 2021;8(2) 34 - 42, doi: 10.37134/jictie.vol8.2.4.2021.

Mascarenhas Neto PT, Araújo WJ. Segurança da informação Uma visão sistêmica para implantação em organizações. Editora UFPB, p. 1-160, 2019.

Neves DLF, Pavani GC, Sales RM, Lopes TSA. A segurança da informação de encontro às conformidades da LGPD. Revista Processando o Saber. 2021;(3) 186-198, eISSN: 2179-5150.

Kessler SR, Pindek S, Kleinman G, Andel AS, Spector P. Information security climate and the assessment of information security risk among healthcare employees. Health Informations Journal. 2019;26(1) 461-473, doi: 10.1177/1460458219832048.

Lopes IM, Guarda T, Oliveira P. General Data Protection Regulation in Health Clinics. Journal of Medical Systems, 2020;44(2), 44-53, doi:10.1007/s10916-020-1521-0.

Gregori, M. S. Os impactos da lei geral de proteção de dados pessoais na saúde suplementar. Revista de Direito do Consumidor, 2020;127(1) 171–196.

Nahai F. General Data Protection Regulation (GDPR) and Data Breaches: What You Should Know. Aesthet Surg J . 2019 Jan 17;39(2):238-240. doi: 10.1093/asj/sjy296.

Iramina A. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. Revista de Direito, Estado e

Telecomunicações, 2020;12(2) 91-117, doi:
<https://doi.org/10.26512/lstr.v12i2.34692>

Costa JM, Rosa SO. Lei Geral de Proteção de Dados Aplicada à Saúde. Revista Humanidades e Inovação, 2021;8(45)

Holanda DA, Mello VVC, Zimmermann RD. Documentação Digital em Odontologia. Odontol. Clin. Cient. 2010;9(2) 111-113. ISSN 1677-3888.

Bruniere LS, Tanaka EE, Ito FA. Proteção da integridade e da autenticidade das radiografias odontológicas digitais. Odontol. Clín.-Cient. 2011;10(3) 211-216. ISSN 1677-3888.

Burgess, J. Digital DICOM in Dentistry. Open Dent J. 2015;31(9) 330-336, doi: 10.2174/1874210601509010330.

Leal MCB, Barreto FSC, Flizikowski EBS, Nascimento WR. O conhecimento dos estudantes sobre direito de imagem do paciente. Revista Bioética. 2018;26(4): 597-605. doi: 10.1590/1983-80422018264278.

Nascimento DB. Análise bioética da utilização de imagens de pacientes em mídias sociais eletrônicas. 2016. 103 f. Dissertação de mestrado (Programa de Pósgraduação em Bioética) – Faculdade de Ciências da Saúde, Universidade de Brasília, Brasília-DF.

Conselho Federal de Odontologia. Resolução n. 196 de 29 de janeiro de 2019. Autoriza a divulgação de autoretratos (selfie) e de imagens relativas ao diagnóstico e ao resultado final de tratamentos odontológicos, e dá outras providências. Disponível em:
<http://sistemas.cfo.org.br/visualizar/atos/RESOLU%C3%87%C3%83O/SEC/2019/196>

Costa MAP, Sarlet GBS. A perspectiva da proteção de Dados pessoais em face dos Direitos das criança e Adolescentes no sistema Normativo brasileiro. In:

Direito, Ambiente e Tecnologia: estudos em homenagem ao professor Carlos A. Molinaro. 2021, 489-511, doi: 1036592/9786587424620.

Garbin CAS, Garbin AJI, Saliba NA, Saliba NA, Zina LG.; Gonçalves E. El consentimiento informado en la clinica odontologica. Acta odontol. Venez., ene. 2007;45(1) 37-43. ISSN 0001-6365.

Sales-Peres SHC, Sales-Peres A, Eleutério ASL, Oliveira JLG, Gigliotti MP. Termo de consentimento livre e esclarecido aos usuários de clínicas odontológicas brasileiras: aspectos éticos e legais. Ciênc. saúde coletiva. 2011 16(1), 805-812, doi: 10.1590/S1413-81232011000700011.

Yarid SD, Batista TS, Silva CA, Luz MN, Ribeiro WE. Uso do termo de consentimento livre e esclarecido (TCLE) por cirurgiões-dentistas em atividades clínicas. Odontol. Clín.-Cient. 2012;11(3) 239-242.

Muniz JO, Hessel T. Segurança de Software para a Área de Saúde: Uma avaliação dos requisitos de segurança aplicada em software de Registro Eletrônico em Saúde. 2019. Trabalho de Conclusão de Curso - Faculdade de Tecnologia de Americana – Ministro Ralph Biasi, São Paulo –SP.

Barbalho R, Postal L; Wazlawick RS. Avaliação da conformidade do e-SUS AB PEC segundo a certificação da SBIS/CFM. In: Simpósio brasileiro de computação aplicada à saúde (SBCAS), 17. 2017, São Paulo. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2017, ISSN 2763-8952. DOI: <https://doi.org/10.5753/sbcas.2017.3705>.

Novaes AL, Vito C, Bousso F, Moribe G, Balthazar L, Kasputis MB, et al. Dados de saúde e a Lei Geral de Proteção de Dados: Estudos de casos, Guia Saúde Bluz. p. 1-46, 2019.

APÊNDICE I – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

**UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS DA SAÚDE
DEPARTAMENTO DE CLÍNICA E ODONTOLOGIA SOCIAL
PROGRAMA DE PÓS-GRADUAÇÃO EM ODONTOLOGIA**

Prezado (a) **PARTICIPANTE DA PESQUISA**

Os pesquisadores **MANOEL PEREIRA DE LIMA** e **MARCELO AUGUSTO OLIVEIRA DE SALES** convidam você a participar como voluntário da pesquisa intitulada **“LEI GERAL DE PROTEÇÃO DE DADOS: ADEQUAÇÕES DOS SERVIÇOS ODONTOLÓGICOS NO BRASIL.”** O objetivo deste estudo é verificar a segurança no gerenciamento de dados pessoais por parte dos cirurgiões-dentistas que trabalhem, armazenem ou processem essas informações.

Após ler as informações a seguir e ao aceitar fazer parte desta pesquisa, marque a opção **“li e estou de acordo com termos do estudo”** para dar continuidade com a participação. Caso não esteja de acordo, o Sr. (a) não será penalizado de forma alguma e poderá optar por não participar. Além disso, também é lhe assegurado o direito de retirar, a qualquer momento, o consentimento sem qualquer penalidade.

Os pesquisadores da pesquisa podem ser contatos a qualquer momento através dos contatos: - Manoel Pereira de Lima, e-mail: manoellimaodonto@gmail.com, cel.: (83) 98188-2400; -Marcelo Augusto Oliveira de Sales, e-mail: marceloxray@gmail.com, cel.: (83) 99900-0538. Além desses, o comitê de ética do Centro de Ciências da Saúde (CEP/CCS/UFPB) pode ser contatado para esclarecimentos de dúvidas pelo e-mail: comitedeetica@ccs.ufpb.br.

Este estudo objetiva avaliar se os cirurgiões-dentistas brasileiros, que manipulam, armazenam e/ou gerencia dados pessoais sensíveis estão seguindo as exigências da LGPD. A participação no estudo se dará através do preenchimento de um questionário on-line, que deve dispende cerca de 5 minutos, contendo perguntas direcionadas ao tema, como: conhecimento da nova

lei, nos métodos de obtenção, armazenamento e compartilhamento de dados pessoais sensíveis, além das demais exigências que se enquadrem na odontologia.

Riscos e Benefícios

Com sua participação nesta pesquisa, o(a) Senhor(a) estará exposto a riscos mínimos como constrangimento em responder algumas das questões, e caso eles venham a ocorrer, serão tomadas as providências cabíveis sob a responsabilidade do (a) pesquisador (a) responsável.

Esta pesquisa tem como benefícios a obtenção de informações a respeito da realidade das entidades prestadoras de assistência odontológica no Brasil, quanto às adequações à LGPD. Além disso, os resultados deste estudo fornecerão informações científicas que serão úteis para a comunidade acadêmica e no desenvolvimento de pesquisas futuras.

Sigilo, Anonimato e Privacidade

O material e informações obtidas podem ser publicados em aulas, congressos, eventos científicos, palestras ou periódicos científicos, sem sua identificação. Serão assegurados o sigilo e a privacidade das informações cedidas, garantido o anonimato e não utilização das informações em prejuízo das pessoas. Além disso, o estudo será suspenso imediatamente ao perceber algum risco ou danos à saúde do sujeito participante da pesquisa, consequente à mesma, não previsto no termo de consentimento;

Os pesquisadores se responsabilizam pela guarda e confidencialidade dos dados, bem como a não exposição individualizada dos dados da pesquisa. Sua participação é voluntária e o(a) Senhor(a) terá a liberdade de se recusar a responder quaisquer questões que lhe ocasionem constrangimento de alguma natureza.

Os dados obtidos na pesquisa serão armazenados e guardados sob responsabilidade do pesquisador principal, por um período mínimo de 05 anos.

Devolutiva dos resultados

Os resultados da pesquisa poderão ser solicitados a partir de término das análises dos dados, por e-mail e/ou contato telefônico. Salta-se que os dados coletados nesta pesquisa somente poderão ser utilizados para as finalidades da

presente pesquisa, sendo que para novos objetivos um novo TCLE deve ser aplicado.

Ressarcimento e Indenização

Lembramos que sua participação é voluntária, o que significa que você não poderá ser pago, de nenhuma maneira, por participar desta pesquisa. De igual forma, a participação na pesquisa não implica em gastos a você. Se ocorrer algum dano decorrente da sua participação na pesquisa, você será indenizado, conforme determina a lei.

O Comitê de Ética em Pesquisa em Seres Humanos (CEP) é composto por um grupo de pessoas que estão trabalhando para garantir que seus direitos como participante sejam respeitados, sempre se pautando pelas Resoluções 466/12 e 510/16 do Conselho Nacional de Saúde (CNS). O CEP tem a obrigação de avaliar se a pesquisa foi planejada e se está sendo executada de forma ética. Em caso de dúvidas relacionadas aos aspectos éticos deste estudo, você poderá consultar o Comitê de Ética em Pesquisa Envolvendo Seres Humanos da UFPB no endereço: Campus I - Cidade Universitária CEP: 58.051-900 - João Pessoa-PB, Tel.: (83) 3216 7791 – e-mail: comitedeetica@ccs.ufpb.br.

ANEXO I – QUESTIONÁRIO DESTINADO AOS CIRURGIÕES-DENTISTAS

1. Cidade	Campo aberto
2. Em que esfera administrativa você trabalha?	Privado Público Público/privado
3. Você fotografa seus pacientes?	Sim Não
4. Você usa imagens de pacientes em mídias sociais?	Sim Não
5. Você sabe o que são dados pessoais?	Sim Não
6. Você conhece a nova Lei Geral de proteção de dados (LGPD) – lei nº 13.709?	Sim Não
7. Você sabia que a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em agosto de 2020?	Sim Não
8. Você sabe a diferença entre dados pessoais e dados pessoais sensíveis?	Sim Não
9. Você coleta dados pessoais sensíveis	Sim Não
10. Você realiza o tratamento de dados pessoais de crianças e adolescentes?	Sim, mas não uso termo de consentimento dos pais e/ou responsáveis Sim, e uso o termo de consentimento dos pais e/ou responsáveis Não
11. O serviço possui dados pessoais, de seus colaboradores e clientes, de forma organizada?	Sim Não
12. Os tratamentos de dados realizados estão devidamente justificados?	Sim Não Não tenho conhecimento
13. Há a coleta e registro de algum tipo de consentimento para utilização dos dados pessoais	Sim Não Não tenho conhecimento

cadastrais no momento da solicitação de envio desses dados?	
14. O titular é informado sobre o que será feito com os seus dados pessoais coletados?	Sim Não
15. Caso o paciente queira saber como seus dados pessoais são tratados, haveria alguma forma de atendê-lo?	Sim Não
16. O serviço possui documentações e práticas relacionadas à gestão da privacidade da informação?	Sim Não
17. As operações de tratamento de dados pessoais estão protegidas?	Sim Não
18. Se sim, como?	Campo aberto
19. Existe algum mecanismo de gestão para prevenir ou minimizar falhas de segurança, como o vazamento de dados?	Sim Não
20. Se sim, como?	Campo aberto
21. Os dados pessoais coletados são compartilhados com terceiros?	Sim Não
22. Você utiliza alguma rede social para compartilhamento de exames de imagens de seus pacientes?	Não WhatsApp Twitter Facebook Instagram E-mail
23. O serviço está preparado para atender à solicitação dos titulares de dados, como exclusão, compartilhamento, armazenamento e outros direitos relacionados as operações de tratamento dos seus dados pessoais?	Sim Não
24. O serviço possui alguma certificação de acreditação em diagnóstico por imagem?	Sim Não
25. Se sim, qual?	
26. Você utiliza algum serviço de acesso à laudos e imagens radiográficas?	Sim Não

27.O serviço utiliza o padrão DICOM para compartilhamento de exames de imagem?	Sim Não
28.Você recebe radiografias pela internet?	Site da Clínica Idoc Cfaz.net Outro
29.Como você visualiza os exames de imagem?	Filme impresso Digital