1. INTRODUÇÃO:

O DBC Patologia Diagnóstica valoriza a confiança depositada por nossos pacientes, colaboradores e parceiros, e está comprometido em garantir a privacidade, a segurança e a transparência em todas as etapas de manuseio dessas informações.

Este documento foi desenvolvido para assegurar que todas as atividades envolvendo o tratamento de dados pessoais e sensíveis estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709/2018, a Resolução da Diretoria Colegiada (RDC) nº 786/2023 da ANVISA e sua alteração pela RDC nº 824/2023, a RDC nº 978/2025 da ANVISA, aplicável aos serviços de análises clínicas, a Resolução CFM nº 2.169/2017 e a Resolução CFM nº 1.823/2007, a RDC nº 222/2018 da ANVISA, referente ao gerenciamento de resíduos de serviços de saúde, e o Código de Defesa do Consumidor (Lei nº 8.078/1990).

Esta política define as diretrizes e práticas adotadas para proteger os dados, promovendo um ambiente seguro e respeitoso em relação aos direitos dos titulares.

2. OBJETIVO:

Este documento tem por objetivos:

a) Assegurar o cumprimento integralmente as disposições da LGPD, adotando medidas para proteger os dados pessoais e sensíveis em todas as operações;
b) Assegurar o cumprimento das disposições da RDC nº 786/2023 da ANVISA e da Resolução CFM nº 2.169/2017, garantindo a gestão adequada de amostras biológicas, laudos e dados de saúde em todas as fases do processo diagnóstico;
c) Estar conforme item específico do processo de acreditação externa (PACQ: GPI 10.015).

3. ABRANGÊNCIA:

Esta política se aplica a todos os envolvidos na prestação de serviços de saúde aos pacientes do DBC Patologia Diagnóstica.

4. DESCRIÇÃO:

4.1. Agentes responsáveis pelo tratamento de dados:

Uma vez estipuladas as medidas preventivas de proteção de dados pessoais e, ainda em atendimento às disposições da Lei Geral de Proteção de Dados, deve-se instituir quem serão as pessoas responsáveis dentro do programa. São, em outras palavras, “chamados agentes responsáveis pelo tratamento das informações”.

O **controlador** é a pessoa natural (física) ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais. Ele será o ocupante do “cargo máximo” dentro da hierarquia de instituição da LGPD e seus princípios. O DBC Patologia Diagnóstica nomeia o seu CEO, Dr. Dennis Baroni Cruz, como controlador dos dados.

O **operador** é a pessoa natural (física) ou jurídica que realiza o tratamento dos dados pessoais em nome do controlador. Ele será o ocupante do "cargo operacional" dentro da hierarquia de instituição da LGPD e seus princípios A diferença em relação ao controlador situação justamente no poder de decisão deste último, a quem se encontra subordinado o Operador para fins deste Programa. O DBC Patologia Diagnóstica nomeia o gerente administrativo, como operador dos dados sensíveis.

O **encarregado** de dados (DPO), conforme Art. 41 da LGPD, é a pessoa natural responsável pela comunicação entre o controlador, os titulares e a ANPD. O DBC Patologia Diagnóstica designa formalmente a Dra. Elisabeth Silveira Baroni, advogada, como encarregada de dados, com apoio técnico do escritório BVK Advogados Associados (contato: bvk@bvk.adv.br e telefone (51) 3715-8786), como encarregado de dados. O escritório jurídico contratado prestará assessoria técnica ao encarregado, mas não substitui a necessidade de designação de uma pessoa natural para esta função, conforme exigido pelo Art. 41 da LGPD.

4.2. Levantamento dos dados sensíveis:

Os dados sensíveis são aqueles que revelam origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicato, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos.

O DBC Patologia Diagnóstica realiza um mapeamento completo dos dados sensíveis que a empresa coleta, processa e armazena, incluindo informações dos pacientes, colaboradores e qualquer outra parte envolvida. Esse levantamento inclui as **fontes de coleta** (prontuários médicos, formulários de consentimento, registros laboratoriais), as **modalidades de armazenamento** (físico, digital, nuvem), os **tipos de dados coletados** e **a finalidade** para a qual cada dado é utilizado.

Após o mapeamento, é conduzida uma análise de risco para identificar vulnerabilidades na coleta, armazenamento e processamento desses dados, considerando os potenciais consequências em caso de vazamento.

O DBC Patologia Diagnóstica utiliza um protocolo de atendimento onde além de informação que serão detalhadas em item específico, incluem um termo de consentimento explícito e informado para a coleta e uso de dados sensíveis, conforme exigido pela LGPD, contendo cláusula específica sobre a possibilidade de **tratamento internacional de dados** (ex.: serviços de nuvem localizados no exterior), sempre com garantias contratuais adequadas.

4.3. Termo de sigilo e de confidencialidade dos colaboradores:

O formulário específico *("FR 019 - Termo de Sigilo e Confidencialidade")* tem como principal objetivo formalizar o compromisso dos colaboradores de proteger as informações confidenciais acessadas durante suas atividades no DBC Patologia Diagnóstica, em conformidade com a LGPD. Isso abrange tanto os dados pessoais dos pacientes quanto informações sensíveis de parceiros comerciais e fornecedores, que devem ser mantidas em total confidencialidade.

Esse termo garante que os colaboradores entendam a gravidade da responsabilidade no tratamento de dados pessoais, protegendo a privacidade dos titulares e prevenindo o uso indevido de informações, como venda ou compartilhamento não autorizado. Também protege o DBC Patologia Diagnóstica contra possíveis penalidades legais decorrentes de falhas no cumprimento da LGPD.

O termo inclui alguns os seguintes pontos chave:

- **Descrição das obrigações:** O colaborador se compromete a não divulgar, compartilhar ou utilizar as informações pessoais dos pacientes, parceiros ou fornecedores para fins que não estejam diretamente relacionados à execução de suas funções profissionais.
- **Restrições de acesso:** O colaborador reconhece que somente deve acessar os dados a que está autorizado e que são necessários para a execução de seu trabalho.
- **Proibição de cópias ou retenção indevida de dados:** O colaborador se compromete a não copiar, transferir ou armazenar dados pessoais fora dos sistemas autorizados pelo DBC Patologia Diagnóstica.
- **Consequências legais e disciplinares:** O termo deve descrever as medidas administrativas, civis e criminais que poderão ser aplicadas caso o colaborador viole as regras de confidencialidade, o que pode incluir advertências, demissão por justa causa e, em casos graves, sanções legais com base na LGPD e outras legislações aplicáveis.

O termo deve ser renovado anualmente ou sempre que houver mudanças relevantes na legislação ou nas políticas internas, em conjunto com treinamentos de atualização, garantindo que todos os colaboradores estejam cientes de suas responsabilidades.

O termo de sigilo e confidencialidade deve estar inserido dentro de um programa mais amplo de treinamento contínuo em segurança da informação e proteção de dados. Esse programa deve incluir os **treinamentos iniciais** (sessões detalhadas de introdução para novos colaboradores, explicando a política de proteção de dados da empresa, como a LGPD afeta suas funções e a importância do sigilo), as **sessões de reciclagem** (treinamentos regulares (anualmente ou sempre que necessário) sobre temas de confidencialidade, uso adequado de sistemas de informação e medidas de segurança cibernética), e **testes e avaliações** (aplicação de testes de conhecimento para avaliar o nível de compreensão dos colaboradores sobre suas obrigações e verificar se os princípios do sigilo estão sendo seguidos adequadamente).

Essas práticas garantem que o Termo de Sigilo e Confidencialidade seja mais do que um documento assinado, mas sim uma ferramenta ativa para promover a segurança da informação e a conformidade com a LGPD no DBC Patologia Diagnóstica.

4.4. Protocolo de atendimento:

O protocolo de atendimento é um documento essencial que serve para formalizar e registrar os serviços prestados pelo laboratório de patologia. Ele tem três funções principais:

- **Transparência**: fornecer ao paciente uma confirmação detalhada de que o atendimento foi realizado, informando quais exames foram solicitados, seus prazos de conclusão e outras informações relevantes.
- **Segurança**: estabelecer um registro formal e claro sobre os dados coletados, o atendimento prestado e as etapas subsequentes do processo, protegendo tanto o paciente quanto o laboratório.
- **Controle**: auxiliar o paciente na administração de seu acompanhamento de saúde, facilitando consultas futuras e possíveis reclamações ou pedidos de revisão.

O protocolo de atendimento contém as seguintes informações:

- **Identificação do paciente:** dados essenciais, como nome completo, número do prontuário ou ID do paciente, devem ser incluídos no protocolo, garantindo que ele seja associado ao atendimento correto.
- **Exames solicitados**: deve haver uma descrição clara dos exames solicitados, para que o paciente saiba exatamente o que foi requisitado e quais serão os próximos passos.
- **Prazo estimado para a entrega dos resultados:** informar ao paciente o tempo previsto para a conclusão dos exames, com orientações sobre como acessar os resultados (online, presencial, via telefone, etc.).
- **Orientações gerais:** Incluir informações práticas como detalhes sobre como proceder em caso de dúvidas, telefones de contato e horários de atendimento para tirar dúvidas ou acompanhar o andamento dos exames.
- **Autenticação**: O protocolo deve ser formalizado com uma assinatura do paciente e/ou responsável, garantindo a validade do documento.

Além do protocolo, é fundamental que os pacientes recebam orientações claras sobre o uso e o acesso aos seus dados e resultados. Essas orientações podem ser feitas de maneira verbal ou por meio de materiais impressos ou digitais, que acompanhem o protocolo. São pontos que devem constar:

- **Acesso aos resultados:** informar ao paciente como ele poderá acessar os resultados dos exames. Isso pode incluir instruções para acessar um portal online, e deve ser garantido que o processo de login seja seguro e confidencial.
- **Proteção dos dados pessoais:** explicar ao paciente que seus dados pessoais e de saúde serão mantidos em total sigilo, em conformidade com a LGPD. Isso reforça a confiança no processo e destaca o compromisso do laboratório com a privacidade.
- **Canal de comunicação:** oferecer ao paciente um canal de comunicação direto (telefone, e-mail, ou portal digital) para que ele possa consultar eventuais dúvidas sobre seus exames, desde o agendamento até a entrega dos resultados.

A emissão do protocolo segue um fluxo operacional padronizado e automatizado para garantir que todos os pacientes recebam suas confirmações de forma rápida e correta. No DBC Patologia Diagnóstica o processo é **automático** (gerado diretamente pelo sistema Pathoweb assim que o atendimento é finalizado, garantindo a agilidade e minimizando o risco de erro humano), **integrado com o prontuário eletrônico** (vinculado diretamente ao prontuário eletrônico do paciente, mantendo os registros organizados e acessíveis tanto para a equipe do laboratório quanto para o paciente) e **disponibilizado em diversos formatos** (o protocolo está disponível tanto em formato físico quanto digital, facilitando o acesso e o armazenamento para o paciente).

Ao emitir o protocolo de atendimento, é fundamental observar boas práticas de segurança para garantir a proteção dos dados pessoais e sensíveis dos pacientes. Isso inclui o **controle de acesso** (o sistema Pathoweb é configurado de forma com que apenas pessoas autorizadas, conforme suas funções dentro do DBC Patologia Diagnóstica, possam emitir e visualizar o protocolo; os colaboradores envolvidos no atendimento devem ter o mínimo necessário de acesso aos sistemas para realizar suas funções), a **criptografia** (é a forma de prevenir interceptações ou acessos não autorizados), a **autenticação do paciente** (ao acessar os resultados online ou outros dados referentes ao atendimento, o paciente deve passar por um processo de autenticação seguro por meio de *login* ou senha conforme as melhores práticas de proteção de dados digitais), e a **política de retenção** (os protocolos emitidos devem seguir a política de retenção de documentos, sendo armazenados pelo tempo necessário para fins de auditoria e, posteriormente, descartados de forma segura, conforme as diretrizes da LGPD).

Emitir um protocolo de atendimento ao final de cada interação não apenas promove transparência e confiança para o paciente, mas também oferece uma série de benefícios ao laboratório como a **rastreabilidade e conformidade** (a emissão do protocolo cria uma trilha de auditoria que documenta todas as interações com o paciente, o que é essencial para a conformidade com a LGPD e com as normas de acreditação externas), a **melhoria no atendimento ao paciente** (ele serve como uma referência clara para o paciente acompanhar seu processo diagnóstico, reduzindo dúvidas e aumentando a satisfação com o serviço prestado), a **minimização de erros e retrabalhos** (ao formalizar o atendimento com um documento claro e detalhado, o laboratório reduz o risco de mal-entendidos, como a realização de exames incorretos ou falhas na comunicação com o paciente).

A emissão do protocolo de atendimento é uma prática essencial para assegurar a transparência, o controle e a proteção dos dados no processo de atendimento do DBC Patologia Diagnóstica.

4.5. Retenção e descarte de dados e de materiais biológicos:

O DBC Patologia Diagnóstica estabelece os seguintes prazos mínimos de guarda para dados e materiais, em conformidade com a legislação vigente e as melhores práticas do setor:

- Laudos, em formato físico ou digital: no mínimo 20 anos (Resolução CFM nº 1.823/2007 e recomendação da Sociedade Brasileira de Patologia;
- Blocos de parafina: no mínimo 10 anos (Resolução CFM nº 1.823/2007 e recomendação da Sociedade Brasileira de Patologia);
- Lâminas patológicas: no mínimo 5 anos (Resolução CFM nº 1.823/2007 e recomendação da Sociedade Brasileira de Patologia);
- Requisições médicas: no mínimo 5 anos (Código de Defesa do Consumidor e normas de Vigilância Sanitária);
- Termos de consentimento LGPD: no mínimo 5 anos após o término do tratamento (LGPD e Código de Defesa do Consumidor);
- Registros de Controle de Qualidade: no mínimo 5 anos (RDC nº 786/2023 da ANVISA);
- Documentos de rastreabilidade de amostras: no mínimo 5 anos (RDC nº 786/2023 da ANVISA).

Após o término dos prazos estabelecidos, o descarte será realizado de forma segura, garantindo a impossibilidade de recuperação dos dados, conforme procedimentos específicos de destruição de documentos físicos e digitais. O descarte de materiais biológicos seguirá as normas de gerenciamento de resíduos de serviços de saúde (RDC nº 222/2018 da ANVISA).

4.6. Acesso aos equipamentos de informáticas e ao sistema Pathoweb:

O acesso aos equipamentos de informática é exclusivo aos usuários devidamente autorizados. Isso significa que todos os dispositivos utilizados no DBC Patologia, como computadores, notebook, e outros equipamentos conectados ao sistema de gestão, estão atualmente protegidos para evitar o uso por pessoas não autorizadas.

Cada colaborador possui um *login* individual e exclusivo para acessar os computadores e sistemas. Esse *login* está protegido por uma senha forte, que seja regularmente atualizada e mantida em sigilo. O uso de senhas compartilhadas é estritamente proibido, pois compromete a segurança e impede a identificação precisa de quem está utilizando o sistema. Cada colaborador tem acesso somente às informações e ferramentas necessárias para realizar suas funções, de acordo com o princípio do "menor privilégio", limitando o risco de acessos indevidos.

Os dispositivos físicos de segurança, como travas de tela automáticas e bloqueios por inatividade, estão configurados para que, após um determinado período de ociosidade, o computador exija a reinserção da senha para ser utilizado novamente. Isso garante que, mesmo que um colaborador se afaste de sua estação de trabalho, o dispositivo não fique vulnerável a acessos não autorizados. Caso o colaborador precise se afastar por um período mais longo, é recomendado que ele faça o *logout* do sistema.

Os equipamentos de informática também estão localizados em áreas seguras, onde o acesso físico é possível de ser controlado pelas câmeras de segurança. Em áreas de atendimento, onde há um fluxo maior de pessoas, os monitores estão posicionados de forma a evitar que terceiros possam visualizar informações sensíveis dos pacientes.

Os dispositivos de armazenamento externo, como pen drives, discos rígidos externos ou qualquer outro tipo de mídia removível, estão sujeitos a controles rigorosos de uso. Essas mídias não devem ser conectadas aos equipamentos do laboratório sem autorização prévia, uma vez que podem representar um risco significativo de perda de dados ou de introdução de *malware*. O uso dessas ferramentas está restrito a equipamentos específicos, sendo monitorado.

O departamento de TI, também responsável pela segurança de dados, possui um sistema de monitoramento contínuo do uso dos equipamentos, de modo a detectar e a impedir tentativas de acesso por usuários não autorizados ou atividades suspeitas. Essa abordagem proativa ajuda a garantir que qualquer tentativa de violação de segurança seja rapidamente identificada e tratada.

4.7. Rastreabilidade dos acessos ao sistema e aos dados dos pacientes:

A rastreabilidade refere-se à capacidade de identificar e registrar todas as ações executadas no sistema, especialmente aquelas relacionadas ao acesso, modificação, visualização ou compartilhamento de informações de pacientes. Isso é crucial para garantir a segurança dos dados e para que, em caso de incidentes ou dúvidas, seja possível auditar e investigar o que ocorreu, quem foi o responsável e quais dados foram acessados. Ala tem como características essenciais e que são seguidas no DBC Patologia Diagnóstica:

- **Identificação única de usuários autorizados:** Cada colaborador que tenha acesso ao sistema do laboratório deve possuir um login individual e intransferível. Essa identificação única assegura que todas as ações executadas no sistema possam ser associadas diretamente a uma pessoa específica. O compartilhamento de credenciais entre colaboradores deve ser expressamente proibido, uma vez que isso compromete a rastreabilidade e pode dificultar a identificação de quem realizou determinadas ações.
- **Autenticação segura e controle de acesso:** Além da identificação única, é necessário implementar métodos de autenticação segura, como senhas fortes e, se possível, autenticação em dois fatores (2FA). Isso reduz o risco de acessos não autorizados, mesmo que as credenciais de um colaborador sejam comprometidas. O sistema deve ser configurado para permitir o acesso apenas aos colaboradores que realmente precisam das informações para realizar suas atividades, com níveis de permissão ajustados conforme as funções desempenhadas. Por exemplo, um recepcionista pode precisar acessar dados cadastrais do paciente, enquanto um técnico de laboratório precisará ver detalhes do exame. Já os médicos e patologistas, responsáveis pelos diagnósticos, terão acesso completo aos resultados e laudos dos exames. Garantir que cada colaborador tenha apenas o nível de acesso estritamente necessário é fundamental para limitar a exposição dos dados.
- **Registro detalhado de ações no sistema (*logs*):** O sistema deve estar configurado para registrar automaticamente todas as interações e atividades realizadas dentro da plataforma, criando o que se chama de logs de acesso. Esses logs devem **registrar informações como** identidade do usuário (*login* único), data

e hora exatas do acesso, tipo de ação realizada (visualização, alteração, exclusão, etc.), dados ou arquivos acessados ou modificados (como laudos, dados cadastrais ou resultados de exames), dispositivo ou local de acesso, se possível (IP, estação de trabalho, etc.). Esses logs são essenciais para garantir a rastreabilidade, permitindo verificar se acessos inadequados foram realizados, detectar alterações indevidas nos dados, ou identificar quaisquer tentativas de uso impróprio das informações.

- **Monitoramento e auditorias regulares:** Além de manter os registros de acesso, é importante a implementação de um sistema de monitoramento regular dos acessos. Isso pode incluir auditorias automáticas e periódicas dos *logs* de acesso para verificar padrões de uso anômalos ou suspeitos. Por exemplo, acessos repetidos a dados sensíveis por colaboradores que não têm justificativa para isso ou tentativas de acessar informações fora do horário de expediente podem ser indicadores de um potencial problema de segurança. A equipe de tecnologia da informação (TI) ou o responsável pela segurança de dados no laboratório deve realizar essas auditorias de forma contínua e, em caso de detecção de qualquer anomalia, deve reportar imediatamente para que ações corretivas sejam tomadas. A equipe de TI deverá fornecer relatórios periódicos, preferencialmente mensais, dos testes de resiliência de rede.
- **Retenção e proteção dos *logs* de acesso:** Os *logs* de acesso devem ser armazenados de forma segura e mantidos por um período mínimo, conforme estipulado pelas regulamentações aplicáveis ou pelas políticas internas do laboratório. Esses registros devem ser protegidos contra alterações ou exclusões não autorizadas. Apenas os administradores do sistema ou pessoal devidamente autorizado deve ter permissão para acessar ou manipular esses logs. Os logs de acesso serão armazenados por no mínimo 2 anos, conforme boas práticas de segurança da informação.
- **Consequências e Responsabilidade:** Os colaboradores devem ser informados de que todos os acessos ao sistema são rastreados e monitorados. Eles também devem estar cientes de que acessos indevidos ou violações de segurança, como o uso de dados de pacientes para fins não autorizados, resultam em sanções disciplinares. Essas penalidades podem variar desde advertências até demissões, dependendo da gravidade da infração, e devem ser previstas na política de proteção de dados da empresa. A clareza sobre a existência desse controle é um fator de dissuasão importante, pois desencoraja o uso impróprio dos dados por parte dos colaboradores.
- **Conformidade com a LGPD:** A rastreabilidade dos acessos também é um requisito essencial para assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD). A LGPD exige que as empresas demonstrem que tomaram medidas apropriadas para proteger os dados pessoais que estão sob sua responsabilidade. A capacidade de auditar e rastrear todos os acessos ao sistema é uma dessas medidas de segurança previstas na legislação. Em caso de uma solicitação de um titular de dados ou de uma investigação por autoridades competentes, a existência de logs de acesso pode ser um fator crucial para

demonstrar que o laboratório agiu conforme as exigências da LGPD e implementou políticas eficazes de controle e segurança dos dados.

A rastreabilidade dos acessos ao sistema e aos dados dos pacientes é um mecanismo central para garantir a segurança e a integridade das informações dentro do DBC Patologia Diagnóstica. Ela envolve a criação de um ambiente de controle no qual cada colaborador possui um login único e individual, onde cada ação realizada no sistema é registrada de forma detalhada, e onde auditorias regulares são realizadas para garantir a conformidade com as normas de segurança de dados. Esses processos não apenas garantem a proteção das informações dos pacientes, mas também protegem o laboratório de riscos legais e de segurança, além de assegurarem que o laboratório esteja em conformidade com as exigências da LGPD.

4.8. Compartilhamento de informações de pacientes:

A confidencialidade das informações dos pacientes é um princípio essencial da ética médica e da legislação de proteção de dados. Por isso, qualquer compartilhamento de dados pessoais deve ser realizado com cautela e apenas nas circunstâncias apropriadas.

- **Autorização expressa e formal:** O compartilhamento de informações de pacientes com terceiros devem sempre ser precedido por uma autorização expressa. Essa autorização deve ser obtida de forma clara e documentada, seja por escrito ou eletronicamente, garantindo que o paciente esteja ciente de que informações serão compartilhadas, com quem e para qual finalidade. A autorização deve incluir elementos como a **identificação do paciente** (nome completo, número do documento de identidade, e outros dados que assegurem a correta identificação da pessoa), a **descrição detalhada dos dados a serem compartilhados** (informações específicas do paciente serão divulgadas, como laudos, resultados de exames, ou dados cadastrais), destinatário das informações (identificar claramente quem receberá as informações) e a finalidade do compartilhamento (propósito pelo qual os dados estão sendo compartilhados). A autorização envio de laudos por e-mail ou aplicativos de mensagens aos profissionais envolvidos diretamente no tratamento do paciente é solicitado no protocolo de atendimento, pois esta prática pode proporcionar um aumento do risco de vazamento dos dados pessoais. No DBC Patologia estes dados constam no protocolo de atendimento e é gerado no sistema Pathoweb um termo de autorização expresso e formal.
- **Exceções à necessidade de autorização:** Embora a regra geral seja que as informações só possam ser compartilhadas com a autorização do paciente, há algumas exceções que devem ser claramente compreendidas: **menores de idade ou incapazes** (a autorização deve ser obtida de um responsável legal o que é crucial para proteger os direitos e a privacidade dos indivíduos que não podem consentir por si mesmos) e **obrigações legais** (investigações policiais, exigências judiciais ou notificações de saúde pública). Nesses casos, a organização deve seguir as diretrizes legais aplicáveis, mas deve também buscar informar o paciente, sempre que possível, sobre a divulgação.
- **Registro de autorizações:** Todas as autorizações obtidas devem ser devidamente documentadas e registradas no sistema PathoWeb, garantindo que

haja um histórico de quais informações foram compartilhadas e com quem. Esse registro deve ser mantido em segurança e acessível apenas a colaboradores autorizados, respeitando a privacidade do paciente.

- **Consequências por violação da política:** A violação da política de não compartilhamento de informações sem autorização expressa pode resultar em sanções disciplinares, que podem variar desde advertências até demissões, dependendo da gravidade da infração. É importante que os colaboradores estejam cientes das consequências de suas ações e do impacto que o compartilhamento inadequado de dados pode ter não apenas sobre os pacientes, mas também sobre a reputação e a integridade do laboratório.

A proibição do compartilhamento de dados sem a autorização expressa e formal protege os direitos dos pacientes e assegura a conformidade com a LGPD, refletindo o compromisso da organização com a privacidade e a segurança das informações pessoais.

4.9. Compartilhamento de dados de saúde:

O DBC Patologia Diagnóstica compartilha dados pessoais de saúde exclusivamente nas seguintes situações, sempre respeitando o princípio da finalidade e as vedações da LGPD:

a) Médicos Solicitantes: Envio de laudos e resultados para fins de diagnóstico e tratamento do paciente. Base Legal: Tutela da saúde (Art. 11, II, f da LGPD). Finalidade: continuidade do cuidado médico.

b) Operadoras de Planos de Saúde: Transmissão de dados para faturamento e autorização de procedimentos. Base Legal: Execução de contrato (Art. 7º, V da LGPD). Finalidade: Cumprimento de obrigações contratuais

c) Empresas de Tecnologia (Sistema *Pathoweb*): Armazenamento e processamento de dados em ambiente de nuvem. Base Legal: Interesse legítimo do controlador (Art. 7º, IX da LGPD). Finalidade: gestão operacional do laboratório. Garantias: contrato de prestação de serviços com cláusulas específicas de proteção de dados, tratando a empresa como operadora

d) Autoridades Sanitárias: Notificação compulsória de doenças e agravos de notificação obrigatória. Base Legal: Cumprimento de obrigação legal (Art. 7º, II da LGPD). Finalidade: Vigilância Epidemiológica.

A autorização de envio de laudos por e-mail ou aplicativos de mensagens deve ser excepcional, sempre com autorização expressa e registrada. A prática preferencial é a disponibilização via portal seguro com autenticação em dois fatores, garantindo maior proteção contra acessos indevidos.

Em conformidade com o Art. 11, §4º da LGPD, o DBC Patologia Diagnóstica declara expressamente que **não compartilha** dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses legalmente previstas para prestação de serviços de saúde em benefício dos titulares dos dados.

4.10. Direitos dos Titulares de Dados:

Em conformidade com os Arts. 17 a 22 da LGPD, o DBC Patologia Diagnóstica garante aos pacientes (titulares) os seguintes direitos:

- Confirmação da existência de tratamento de seus dados pessoais;
- Acesso aos dados pessoais tratados pelo laboratório;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa;
- Eliminação dos dados pessoais tratados com consentimento do titular, exceto nas hipóteses de guarda obrigatória;
- Informações sobre as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento nos casos em que o tratamento é baseado no consentimento.

As solicitações referentes aos direitos dos titulares devem ser direcionadas ao **encarregado de dados** através do e-mail bvk@bvk.adv.br ou telefone (51) 3715-878, com prazo de resposta de até 15 dias corridos.

4.11. Treinamento dos colaboradores:

Treinar e desenvolver os colaboradores é a melhor forma de preparar-se para lidar com os desafios de suas rotinas, além de atualizá-los como mudanças impostas pela legislação ou pelo mercado.

Esta visão deve ser dedicada para a implementação e aplicação dos princípios e conceitos da LGPD, até mesmo porque, diante da constante evolução das rotinas e práticas laboratoriais, é natural que a política passe por atualizações.

O treinamento aumenta a eficácia dos objetivos da empresa, dentre eles a instituição de métodos de preservação de sigilo quando do tratamento de dados pessoais.

É realizado um treinamento para cada novo colaborador da empresa e um treinamento anual com todos os colaboradores sobre a LGPD e suas aplicações práticas no DBC Patologia Diagnóstica.

Nestes treinamentos são abordadas as seguintes práticas a ser adotadas pelos colaboradores:

a) Aplicação do termo de sigilo e de confidencialidade aos colaboradores:

O formulário específico *("FR 019 - Termo de Sigilo e Confidencialidade")* deve ser assinado por todos os colaboradores no **momento da admissão**, como parte do

processo de integração inicial (*onboarding*), garantindo que, antes de iniciar qualquer atividade no DBC Patologia Diagnóstica, o colaborador tenha ciência e concorde formalmente com as obrigações impostas. Uma **cópia assinada do termo deve ser arquivada**, mantendo registros formais que possam ser auditados a qualquer momento, especialmente em casos de inspeção de conformidade ou em auditorias de acreditação. Ele deve ser **renovado periodicamente** e inserido nos **treinamentos**, **reciclagens** e **testes/avaliações** conforme previamente mencionado. Além disso, treinamentos anuais sobre LGPD, segurança da informação e confidencialidade serão realizados, além de simulações de incidentes (*tabletop exercises*).

b) Acesso aos equipamentos de informática da empresa e do sistema PathoWeb:
No treinamento sobre o acesso aos equipamentos de informática e ao sistema Pathoweb, os colaboradores devem ser instruídos a utilizar exclusivamente seus *logins* e senhas individuais para acessar os computadores e sistemas da empresa, garantindo que cada acesso seja devidamente identificado e rastreável. Senhas fortes devem ser criadas e mantidas em sigilo, sendo proibido o compartilhamento entre os colaboradores. Equipamentos de informática devem ser protegidos com bloqueio automático de tela em caso de inatividade, e os colaboradores devem garantir que, ao se ausentarem, façam logout ou bloqueiem o dispositivo. O uso de mídias externas, como pen drives, só deve ser realizado com autorização prévia, para evitar riscos de segurança. A equipe de TI monitorará os acessos e atividades no sistema, assegurando que apenas os colaboradores autorizados tenham acesso aos dados sensíveis, conforme as exigências da LGPD.

c) Solicitar apenas dados essenciais dos pacientes:
Os colaboradores devem solicitar apenas os dados pessoais necessários para a realização dos serviços diagnósticos. A coleta de dados deve seguir o princípio da minimização, conforme previsto na LGPD, ou seja, apenas as informações estritamente necessárias para atingir o objetivo do diagnóstico e do tratamento devem ser solicitadas, evitando o excesso de dados e reduzindo o risco de exposição indevida.

d) Evitar a prática de arquivar cópias de documentos de identidade dos pacientes:
A manutenção de cópias físicas ou digitais de documentos de identidade deve ser evitada, pois isso aumenta os riscos de exposição indevida de dados sensíveis. O armazenamento de documentos deve ser justificado por necessidade legal ou contratual, sendo preferível validar as identidades sem arquivar cópias, sempre que possível.

e) Emissão do protocolo de atendimento e orientações gerais ao final de cada atendimento:
Após realizar o cadastro do paciente e dos exames no sistema Pathoweb, é fundamental verificar se todos os dados estão corretos e atualizados, incluindo informações pessoais, tipo de exame e detalhes do atendimento. Essa verificação é crucial para evitar erros antes de emitir o protocolo. Em seguida, o protocolo é gerado automaticamente pelo sistema Pathoweb, que preencherá os dados do paciente, os

exames solicitados, o número do protocolo e o prazo estimado para a entrega dos resultados. O colaborador deve imprimir o protocolo ou, caso o paciente prefira, enviá-lo por e-mail ou disponibilizá-lo no portal online seguro, de acordo com as diretrizes de segurança de dados. É importante garantir que o paciente compreenda todas as informações contidas no protocolo, incluindo os exames solicitados e os prazos estimados. Após a entrega do protocolo, o colaborador deve fornecer orientações detalhadas sobre os próximos passos. Isso inclui informar o prazo de entrega dos resultados e como o paciente poderá acessá-los, seja online, por e-mail ou presencialmente. Além disso, o paciente deve ser orientado sobre como acompanhar o andamento do exame e os canais de comunicação disponíveis, como telefone, e-mail ou portal online. Durante todo o processo, o colaborador deve garantir a proteção da privacidade do paciente, assegurando que os dados de outros pacientes não estejam visíveis. O paciente deve ser informado de que o DBC Patologia Diagnóstica segue rigorosas regras de sigilo e proteção de dados, com acesso restrito aos profissionais autorizados. Se o paciente tiver dúvidas sobre o exame ou o protocolo emitido, o colaborador deve esclarecer de forma clara e objetiva, sem fornecer informações médicas específicas ou resultados preliminares que não estejam sob sua responsabilidade. Dúvidas mais complexas devem ser encaminhadas ao responsável técnico. É essencial que o colaborador seja paciente e claro ao explicar as orientações, especialmente para pacientes que não estejam familiarizados com o processo ou com o uso de tecnologia. Documentar quaisquer instruções adicionais fornecidas ao paciente também é uma prática recomendada para garantir que todas as informações necessárias foram devidamente passadas. Incentivar sempre o paciente para tomar conhecimento der seus laudos mediante acesso no site institucional do DBC Patologia Diagnóstica, por meio de senha pessoal e *login*, procedimento que, por norma, “elimina” a interferência do profissional de atendimento nessa fase do processo. Por fim, é importante que a emissão do protocolo e as orientações sejam realizadas de maneira consistente para todos os pacientes, garantindo a conformidade com as políticas de segurança e a Lei Geral de Proteção de Dados (LGPD).

f) Confidencialidade e autorização no tratamento de dados pessoais dos pacientes:

Os colaboradores devem ser constantemente treinados e sensibilizados sobre a importância de manter a confidencialidade dos dados dos pacientes. Devem entender que o vazamento de informações pode resultar em consequências legais, além de prejudicar a confiança do paciente na instituição. Os colaboradores devem ser instruídos sobre como lidar com solicitações de informações de terceiros e a importância de sempre verificar a validade da autorização antes de compartilhar qualquer dado. Deve ser enfatizado a importância da autorização no tratamento de dados pessoais dos pacientes. Todos devem estar cientes de que é estritamente proibido usar, divulgar ou facilitar o acesso a informações sensíveis sem a devida autorização. Além disso, nenhuma informação sobre pacientes deve ser fornecida a terceiros sem uma autorização expressa e formal, exceto em casos de menores de idade ou incapazes, onde a proteção dos dados é ainda mais crítica. É fundamental que cada colaborador assuma a responsabilidade de preservar a privacidade dos

dados e respeitar a legislação vigente, garantindo assim a confiança dos pacientes no nosso trabalho.

g) Orientações gerais

Os colaboradores do setor de recepção/atendimento devem ser orientados a não comentar, analisar ou emitir quaisquer opiniões acerca do conteúdo do laudo, mesmo quando solicitado pelo paciente. Nestas hipóteses, o paciente deverá ser atendido por profissional qualificado, de forma individualizada e em ambiente privativo (preferencialmente o seu médico assistente ou solicitante do exame).

4.12. Indicadores de gestão de dados:

O DBC Patologia Diagnóstica monitorará continuamente, com revisões periódicas, indicadores de eficácia das práticas de proteção de dados como:

- **Número de solicitações de acesso de titulares de dados**.
- **Taxa de cumprimento de solicitações de correção de dados**.
- **Incidentes de segurança registrados** (ex: tentativas de acesso não autorizado).
- **Tempo médio de resposta às solicitações dos titulares;**
- **Número de incidentes reportados à ANPD;**
- **Índice de conclusão de treinamentos obrigatórios em LGPD.**

Deverão ser produzidos relatórios que contenham a análise dos indicadores acima, permitindo a identificação de áreas de melhoria e a tomada de decisões estratégicas.

A realizar de capacitações regulares para a equipe sobre a importância da proteção de dados e como os indicadores deverão ser usados para melhorar a gestão de informações.

4.13. Relação com terceiros:

É bastante comum que pessoas físicas ou jurídicas, prestadoras ou tomadoras de serviços junto ao DBC Patologia Diagnóstica, acabem por ter acesso a dados pessoais de pacientes. Como o laboratório, em si, é o controlador dos dados, pois a ele foram confiados, se tem que a responsabilidade se estende, inclusive, para os casos em que a violação ocorre por má prática destes terceiros.

São atividades envolvidas: setores de contabilidade, setores jurídicos, empresas de manutenção de equipamentos, empresas de manutenção predial, empresas de prestação de serviços de limpeza e asseio, empresas de prestação de serviços de segurança, empresas de tecnologia da Informação, operadoras de planos de saúde, administradoras de convênios, secretarias municipais e estaduais da saúde, clínicas de medicina do trabalho, empregadores dos pacientes, entre outros.

Pela unânime interpretação das disposições da LGPD, é de responsabilidade do DBC Patologia Diagnóstica o acesso a dados pessoais de pacientes por parte de terceiros.
Todos os prestadores e tomadores de serviços antes relacionados têm condições, em algum momento da relação contratual, de acessar – ou ao menos visualizar – documentos que contenham informações sigilosas. Desta forma deve-se:

- Envidar esforços no sentido de limitar ao absolutamente necessário o acesso a dados pessoais de pacientes por parte dos prestadores de serviços, seja ao frequentarem o ambiente laboratorial, seja pela análise de documentos essenciais para a consecução do quanto contratado.
- No dia a dia da relação contratual com tomadores de serviços, aqueles que pagam pelos exames, deve-se disponibilizar tão somente a documentação minimamente necessária.
- Não envie quaisquer dados que não sejam efetivamente solicitados e cuja disponibilização seja pertinente.
- Antes de qualquer outra providência, o laboratório é jungido pelo dever máximo de sigilo, e a LGPD veio a consolidar esta condição: não viole zele para que não seja violado o seu compromisso.
- Em todos os contratos firmados com terceiros, será inserida cláusula de compromisso com a LGPD. Além disso, os prestadores considerados críticos poderão ser submetidos a auditorias periódicas de conformidade em proteção de dados, como medida de *due diligence*.

4.14. Plano e mecanismo para a destruição dos registros:

O plano e mecanismo para a destruição dos registros no contexto do DBC Patologia Diagnóstica deve seguir as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) e outras regulamentações pertinentes à área de Patologia.

A destruição de dados sensíveis deve ser realizada de forma segura e eficiente, garantindo que não haja possibilidade de recuperação dos registros.

O tempo de armazenamento de cada tipo de material é variável, sendo os registros que envolvem a LGPD incluem as seguintes situações:
a cópia

- cópia virtual/digital do laudo impresso: arquivada de forma permanente;
- documentos digitalizados: os pedidos devem ser guardados por vinte (20) anos;
- documentos digitalização com nível de segurança nível 2: descartados imediatamente após seu uso, entretanto, a Sociedade Brasileira de Patologia sugere que guarda seja de cinco (5) anos;
- outros documentos extras (segundas vias de requisições, cópias de identidades vinda de outros serviços, laudos impressos internamente para revisão, etiquetas de exames de frascos com o material biológico que foi descartado): descartados imediatamente após o uso.

A forma de descarte destes registros físicos é através de fragmentadoras/trituradoras de papel, impossibilitando sua identificação.

Para dados eletrônicos, serão adotadas técnicas conjuntas com a empresa de TI e com o *PathoWeb* que garantam a impossibilidade de recuperação, como a sobrescrição ou a utilização de *software* específico para destruição de dados. O registro do processo de

destruição destes dados deverá documentar cada etapa com data, método, responsável e lista dos dados destruídos, além de ser mantido permanentemente, em conformidade com as práticas de auditoria e de fiscalização.

Serão realizadas revisões periódicas deste plano, ajustando-o conforme mudanças na legislação, nas operações do laboratório ou nas práticas de gestão de dados.

4.15. Plano de contingência para eventos de vazamento de dados:

Constitui um evento de vazamento de dados, incluindo acessos não autorizados, perda de dispositivos de armazenamento, e divulgação inadequada de informações.

A estratégia de resposta inclui o desenvolvimento de estratégia de resposta a incidentes que inclua **procedimentos de contenção** para minimizar o impacto do vazamento e a **avaliação da gravidade do incidente** e da natureza dos dados afetados.

O protocolo de comunicação deverá incluir a **notificação aos titulares de dados afetados**, a **comunicação à Autoridade Nacional de Proteção de Dados (ANPD)** conforme exigido pela LGPD e **comunicação interna** para manter a equipe informada sobre o incidente e os passos que estão sendo tomados.

Além dos treinamentos regulares, serão realizados **exercícios simulados de incidentes (*tabletop exercises*)**, para capacitar a equipe a responder a potenciais vazamentos de dados.
Após a ocorrência de um incidente, serão revisadas as respostas e identificadas oportunidades de melhoria no plano de contingência e nas práticas de proteção de dados.

4.16. Gestão de incidentes de segurança:

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados, o DBC Patologia Diagnóstica seguirá o seguinte protocolo:

1. Contenção imediata do incidente e avaliação dos danos;
2. Comunicação à ANPD em até 72 horas, conforme Art. 48 da LGPD;
3. Notificação aos titulares afetados quando aplicável;
4. Documentação completa do incidente;
5. Revisão e melhoria dos controles.

O encarregado de dados será o responsável por coordenar a resposta a incidentes e as comunicações com a ANPD e titulares afetados.

4.17. Providências em relação ao colaborador:

A violação quanto aos dados pessoais, através de seu tratamento não responsável deverá acarretar, desde que comprovada, a adoção de medidas em relação ao colaborador infrator. Uma vez que estejam os colaboradores compromissados quanto ao dever de sigilo, assim como treinados no que tange aos princípios e preceitos da LGPD,

passará a se constituir em obrigação do contrato de trabalho a observância de todos os elementos necessários à preservação dos dados pessoais.

Nesta via, sob pena de conivência por parte do empregador, deverá o Controlador de Dados, por meio de seu Operador, fazer impor as medidas punitivas legais quando comprovada a autoria do ilícito laboral, através do enquadramento no rol de faltas graves do obreiro:

- A previsão legal do respeito ao sigilo profissional e a consequência de sua quebra estão no artigo 482, letra "g", da Consolidação das Leis do Trabalho (CLT): ***Art. 482:*** *Constituem justa causa para rescisão do contrato de trabalho pelo empregador: (...); g) violação de segredo da empresa.".*

- Mas é claro, nem toda má prática resulta em prejuízos ao laboratório ou ao paciente. No entanto, as pequenas falhas e quebras de rotina devem ser igualmente apontadas, relatadas e objeto de providências pelo Controlador e Operador de dados.
- Após avaliação conjunta da postura e atuação do colaborador em relação ao evento danoso ao sigilo de dados pessoais, assim como das eventuais consequências, deverão Controlador e Operador recomendar ao Setor de Recursos Humanos a avaliação da aplicação de:

a) Advertência: É o modo mais leve de punir o colaborador que desrespeita as regras da empresa. É por meio dessa ferramenta que o empregador avisar ao seu funcionário que ele fez algo de errado e que, em caso de reincidência, o seu contrato poderá ser rescindido por justa causa.

b) Suspensão: é a punição pertinentes aos casos de cometimento de falta de natureza mediana ou nas hipóteses em que o empregador já advertiu por escrito, permanecendo o colaborador na prática de faltas em relação ao tratamento dos dados pessoais.

c) Demissão por justa causa: Inicialmente, deve-se relembrar o preceito de que a falta cometida pelo empregado, para fins de justa causa, deve ser de tal gravidade que justifique a quebra da necessária confiança ao prosseguimento do contrato de trabalho. Assim, para que haja essa penalidade, deve-se: ou se estar diante de uma situação realmente grave, ou, tratar-se de empregado reincidente, já advertido e suspenso em momentos anteriores ou em caso de reincidência (previamente advertido e suspenso).

5. GLOSSÁRIO:

Acesso aos Equipamentos de Informática: Regras e diretrizes que garantem que os colaboradores utilizem seus próprios logins e senhas para acessar sistemas e dispositivos da empresa, mantendo a rastreabilidade.

Acreditação Externa: Processo pelo qual uma organização é avaliada por uma entidade externa em relação a padrões de qualidade e conformidade. O DBC Patologia Diagnóstica segue os requisitos do PACQ (Programa de Acreditação e Qualidade).
Auditoria de Conformidade: Processo de verificação e avaliação para garantir que as práticas da organização estejam alinhadas com a legislação e políticas de proteção de dados.
Autorização Expressa e Formal: Consentimento claro e documentado do paciente para o compartilhamento de seus dados pessoais, incluindo identificação do paciente, dados a serem compartilhados, destinatário e finalidade do compartilhamento.
Confidencialidade: O princípio de manter informações pessoais e sensíveis em sigilo, evitando sua divulgação não autorizada a terceiros.
Controlador: A pessoa natural ou jurídica que toma as decisões referentes ao tratamento de dados pessoais. No DBC Patologia Diagnóstica, é o CEO, Dr. Dennis Baroni Cruz.
Dados Pessoais: Qualquer informação relacionada a uma pessoa natural identificada ou identificável, como nome, CPF, endereço, entre outros.
Dados Sensíveis: Informações que, se divulgadas, podem causar discriminação ou constrangimento ao titular, como dados sobre saúde, origem racial, convicções religiosas, entre outros.
Descarte de Documentos: Processo de eliminação de documentos que contenham informações sensíveis, garantindo que não possam ser recuperadas após o descarte.
Encarregado: pessoa natural designada como DPO, com apoio técnico do escritório jurídico contratado.
Lei Geral de Proteção de Dados Pessoais (LGPD): Legislação brasileira (Lei nº 13.709/2018) que estabelece normas para a proteção de dados pessoais, visando garantir a privacidade e os direitos dos titulares.
Medidas Preventivas: Ações adotadas para proteger os dados pessoais e sensíveis, garantindo que o tratamento esteja em conformidade com a LGPD.
Monitoramento de Acessos: Acompanhamento das atividades dos colaboradores no sistema para garantir que somente pessoas autorizadas tenham acesso a informações sensíveis.
Operador: A pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. No DBC Patologia Diagnóstica, o gerente administrativo, Julio Cézar Silveira, é designado como operador.
Penalidades Legais: Consequências jurídicas que podem ser aplicadas em caso de violação da LGPD, incluindo advertências, multas, e ações civis ou criminais.
Prestadores de Serviços: Terceiros que, no curso de suas atividades, podem acessar dados pessoais de pacientes, incluindo empresas de manutenção, segurança e tecnologia da informação.
Princípio da Minimização: Diretriz da LGPD que estabelece que apenas dados pessoais estritamente necessários para a realização de um serviço devem ser coletados.
Protocolo de Atendimento: Documento que registra informações sobre a prestação de serviços, como dados do paciente, exames solicitados e prazos para entrega de resultados.
Registro de Autorizações: Documentação sistemática que mantém um histórico de quais informações foram compartilhadas, com quem e sob qual autorização.
Registro Formal: Documentação que comprova a obtenção de autorização ou o cumprimento de obrigações legais, mantendo um histórico de ações realizadas.
Responsável Legal: Pessoa designada para consentir em nome de indivíduos incapazes (como menores de idade) em questões que envolvem a autorização de compartilhamento de dados.

Segurança da Informação: Conjunto de práticas e tecnologias para proteger os dados pessoais contra acesso não autorizado, vazamentos e outras ameaças.
Termo de Sigilo e Confidencialidade: Documento formal que estabelece o compromisso dos colaboradores em proteger as informações confidenciais acessadas durante suas atividades, conforme a LGPD.
Titular dos Dados: Pessoa a quem se referem os dados pessoais, que possui direitos em relação às suas informações.
Treinamento Contínuo: Programa de capacitação que visa manter os colaboradores informados e atualizados sobre suas responsabilidades em relação à proteção de dados e segurança da informação.
Treinamento de Colaboradores: Programa educativo destinado a capacitar os funcionários em relação às normas de proteção de dados e à confidencialidade das informações dos pacientes.
Violação de Dados: Qualquer ato que comprometa a segurança das informações pessoais, resultando em acesso, uso ou divulgação não autorizados.

6. REFERÊNCIAS:

ASSIS, EMILIO. Manual de Boas Práticas em Patologia/Emilio Assis. São Paulo: Sociedade Brasileira de Patologia, 2020.

BRASIL. Agência Nacional de Vigilância Sanitária (ANVISA). Resolução da Diretoria Colegiada - RDC n.º 978, de 6 de junho de 2025. Dispõe sobre o funcionamento de Serviços que executam as atividades relacionadas aos Exames de Análises Clínicas (EAC). Diário Oficial da União. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-anvisa-n-978-de-6-de-junho-de-2025-635044217. Acesso em: 30 jul. 2025.

BRASIL. Agência Nacional de Vigilância Sanitária (ANVISA). Resolução da Diretoria Colegiada - RDC n.º 824, de 26 de outubro de 2023. Altera a Resolução de Diretoria Colegiada - RDC n.º 786, de 5 de maio de 2023, que dispõe sobre os requisitos técnico-sanitários para o funcionamento de Laboratórios Clínicos, de Laboratórios de Anatomia Patológica e de outros Serviços que executam as atividades relacionadas aos Exames de Análises Clínicas (EAC) e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, n. 205, p. 70, 27 outubro 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-rdc-n-824-de-26-de-otubro-de-2023-519173273 Acesso em: 30 jul. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 jul. 2025.

CRUZ, PÉRICLES GÓES DA (COORD.). Manual para organizações prestadoras de serviço de saúde - OPSS: roteiro de construção do manual brasileiro de acreditação ONA 2022/Coordenação Científica: Péricles Góes da Cruz; Gilvane Lovato. Edição especial - Brasília: ONA, 2021.

MARINHO, LARISSA CARDOSO (COORD.). Programa de Acreditação e Controle da Qualidade da Sociedade Brasileira de Patologia – PACQ-SBP: Rol de Requisitos para Acreditação - RRA - São Paulo, SP: Sociedade Brasileira de Patologia - SBP, 2023.

ROCHA, ADRIANA; GOULART, BRUNO KILPP; ABUD, JAMILE; SCHAEFER, PEDRO GUILHERME; GUTKOSKI, SIMONE; MACHADO, SIMONE MÁRCIA DOS SANTOS. Manual da Qualidade: Patologia em Foco. Porto Alegre, RS: Sociedade Brasileira de Patologia - SBP, 2021.

Disponível em: https://www.sbp.org.br/wb/wp-content/uploads/2021/12/Manual-de-Patologia_Porto-Alegre.pdf. Acesso em: 30 jul. 2025.