SANTA CASA DE PARANAVAI
PLANO DIRETOR DE PRIVACIDADE (PDP)

Nome do documento:	Plano diretor de privacidade (PDP)
Versão	1.0
Autor	Gilberto Lisboa
Data de criação	02/12/2022

Histórico do documento

Versão	Data	Descrição	Autor
1.0	02/12/2022	Documento Inicial	Gilberto Lisboa

VISÃO GERAL

A DPO Serviços juntamente com a Giozet e Afonso organizaram este plano diretor com o objetivo de estabelecer o planejamento para adequação completa da Santa Casa de Paranavaí a LGPD atendendo aos aspectos técnicos e jurídicos.

O objetivo

É fundamental para a Santa Casa de Paranavaí atender a legislação para garantir sua confiabilidade diante dos diversos publicos que atende e para evitar multas e sanções.

- Quando questionado ser capaz de demonstrar que respeita a lei de privacidade
- Credibilidade (ser reconhecido) pelos clientes dos profissionais e pacientes
- Ter a equipe treinada e consciente sobre a legislação de privacidade

INTRODUÇÃO

Em organizações ligadas a prestação de serviços em assistencia a saude como em nosso caso na Santa Casa de Paranavai o gerenciamento da privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que o hospital deve prover para conquistar a confiança dos pacientes, acompanhantes, e colaboradores tanto administrativos quanto da equipe assistencia, e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade.

Nosso Plano Diretor de Privacidade (PDP) busca garantir os mecanismos necessários para garantir a Governança em Privacidade (GP) capturando os requisitos de privacidade para definir como os dados pessoais, especialmente em nosso caso dos pacientes, mas não limitados a esses, serão manuseados no seu ciclo de vida como um todo.

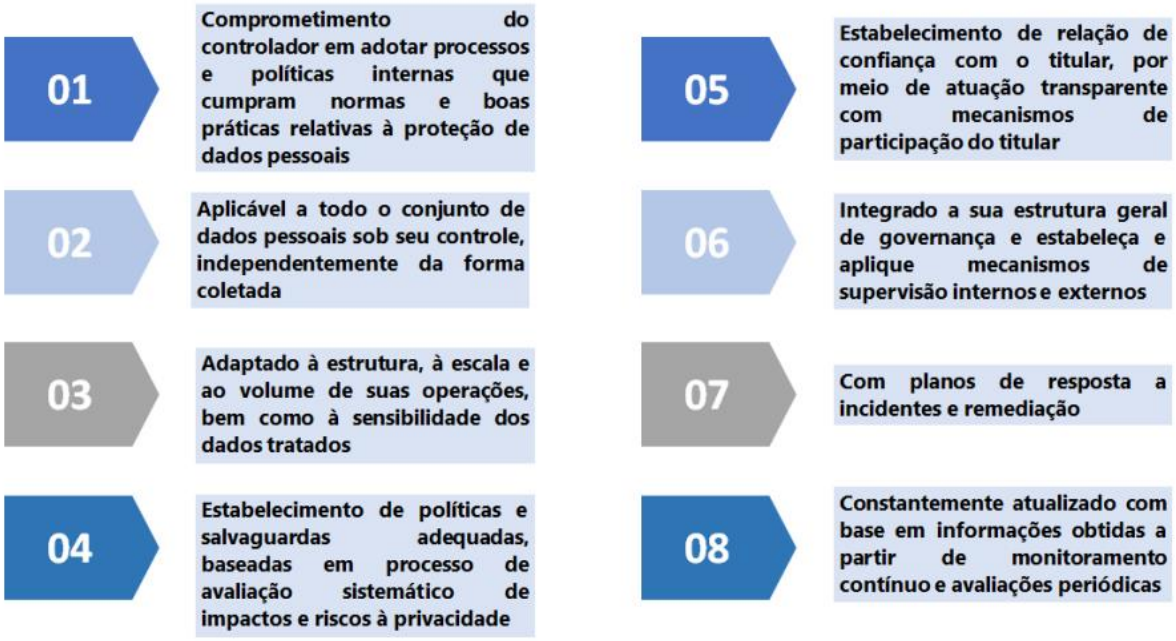
O gerenciamento de segurança e risco, bem como seus respectivos responsáveis, precisam respeitar requisitos complexos e restritivos a serem cumpridos para se ter, assim, uma efetiva governança de privacidade e manuseio de pessoais ao longo de seu ciclo de vida.

A implementação deste Plano Diretor de Privacidade (PDP) é necessária para gerenciar riscos crescentes nas mais variadas áreas.

Cabe aos gestores representados pelo Comite de Privacidade já formado o gerenciamento de segurança e risco para assegurar que o uso dos dados pessoais seja granular, com finalidades específicas e com riscos mapeados e sob controle.

1 – PLANO DIRETOR DE PRIVACIDADE (PDP)

1.1 – O que é A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), em sua Seção II, Das Boas Práticas e da Governança, informa, no Art. 50 § 2º sobre as características mínimas de um Plano Diretor de Privacidade (PDP) – PROJETO DE ADEQUAÇÃO



Diante das características de um Plano Diretor de Privacidade (PDP) – PROJETO DE ADEQUAÇÃO apresentadas pela LGPD é necessário também destacar seus principais atores:

A. Titular, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso III do art. 2º da Lei Geral de Proteção de Dados), em nosso caso trata-se dos pacientes, acompanhantes, funcionários, equipe assistencial, alunos e qualquer outra pessoa física que seja necessário a registro de seus dados.;

B. Controlador, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º da Lei Geral de Proteção de Dados). O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador, em nosso caso a própria Santa Casa;

C. O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII do art. 5º da Lei Geral de Proteção de Dados). Ambos, controlador e operador, recebem a nomeação de “agentes de tratamento” (inciso IX do art. 5º da Lei Geral de Proteção de Dados), em nosso caso são laboratórios, outras empresas envolvidas no processo assistencial como planos de saúde, até mesmo os órgãos publicos que recebem notificações compulsórias, empresas que fornecem benefícios aos funcionários entre outros;

D. O encarregado corresponde a uma pessoa natural inequivocamente investida nessa função (que, na legislação europeia, corresponde ao Data Protection Officer - DPO). Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD - (inciso VII do art. 5º da Lei Geral de Proteção de Dados); Autoridade Nacional de Proteção de Dados - ANPD tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados, desde outubro de 2022 a empresa DPO serviços juntamente com a Giozet e Afonso assumiram este papel e responsabilidade.

Ao contrário de um projeto, que tem início, meio e fim, um programa estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade.

Pode-se, entretanto, criar projetos para se alcançar objetivos do programa. Na criação de projetos para se alcançar objetivos do programa, deve-se selecionar a metodologia mais adequada a realidade institucional.

É necessário definir:

A. os objetivos, as metas e os indicadores;

B. os participantes do comite, a saber: líderes responsáveis por cada frente de atuação do projeto (interação com os funcionários, pacientes, acompanhantes, etc. – Titulares dos dados), operações de TI, segurança, jurídico, operadores, entre outros); e canais de comunicação com os titulares, com os operadores e também com a Autoridade Nacional de Proteção de Dados - ANPD.

1.2 – Estruturação

A estrutura do PROJETO DE ADEQUAÇÃO apresentada neste documento é inspirada no ciclo PDCA (Plan, Do, Check e Act) bem como nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

O programa foi estruturado nas seguintes etapas:

i. Iniciação e planejamento
ii. Implementação em fases
iii. Monitoramento e melhoria contínua

2 – ETAPAS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

2.1 – Iniciação e Planejamento

A etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Com isso em mente, essa etapa é constituída pelos marcos abaixo, que serão detalhados a seguir.

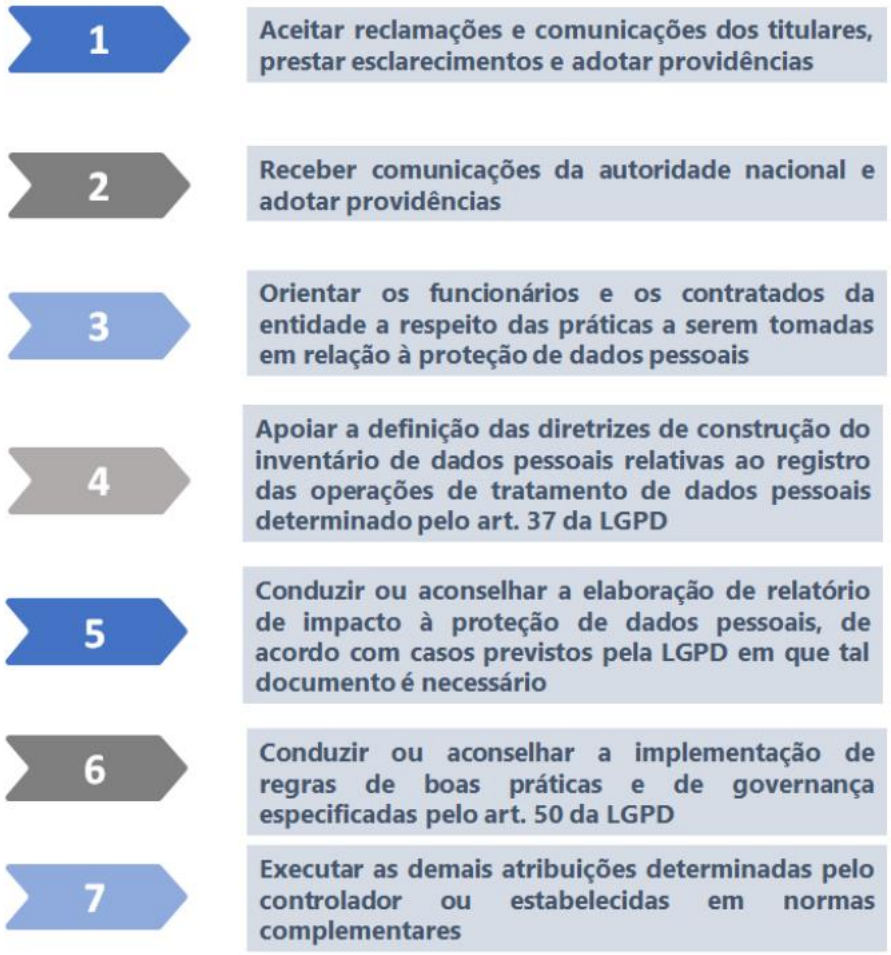
i. Nomeação do DPO – Encarregado de Proteção de Dados
ii. Alinhamento das Expectativas com a Alta Administração
iii. Análise da Maturidade – Diagnóstico do atual estágio de adequação a LGPD
iv. Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna
v. Instituição de estrutura organizacional para governança e gestão de dados pessoais
vi. Inventário de dados pessoais
vii. Levantamento dos contratos relacionados a dados pessoais

Como boa prática já contratada e implementada iniciamos o projeto com a nomeação do Encarregado, que está conduzindo a instituição, em conjunto com o Comitê.

2.1.1 – O Encarregado

A indicação do encarregado deve acontecer no início do projeto de adequação. Atendendo o Art. 5º inciso VIII da LGPD, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Entre as competências de um encarregado apresentadas na LGPD, pode-se citar:



Além das competências elencadas pela LGPD, foi opção da Santa Casa de Paranavai, contratar empresa especializada com metodologia, experiência, conhecimentos e formação para o desempenho da função de encarregado. A terceirização dessa atividade garante independência para sugerir as melhores opções para aplicação de recursos e as ações necessárias, bem como o pronto apoio aos setores no atendimento das solicitações de informações em relação às operações de tratamento de dados pessoais.

O encarregado deverá ter amplo acesso a estrutura organizacional, investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas.

Para garantir o resultado esperado é fundamental o apoio da alta administração é essencial para o sucesso do trabalho executado pelo encarregado, incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros.

Diante da nítida importância do encarregado para a implementação da LGPD e, consequentemente, para o PROJETO DE ADEQUAÇÃO, a seguir é apresentada uma proposta de tópicos a serem abordados, analisados e tratados pelo encarregado.

Nossa abordagem apresenta o trabalho a ser executado pelo encarregado dividido em etapas e os seguintes passos são sugeridos:

Encarregado - Etapa de Iniciação e Planejamento

i. Alinhamento de expectativas entre o encarregado e a diretoria da Santa Casa de Paranavai da Santa Casa de Paranavaí;
ii. Apresentação, para as secretarias da Santa Casa de Paranavaí (secretários, diretores e coordenadores), do papel exercido pelo encarregado como relevante e influenciador;
iii. Como o encarregado pode servir e agregar valor a Santa Casa de Paranavaí, dado o disposto na LGPD;
iv. Confirmar e garantir aos colaboradores da Santa Casa de Paranavaí que, enquanto representante interno da ANPD, seu papel deve ser uma assistência de grande valor e não um obstáculo;
v. Priorização e foco em melhorias, tendo consciência da estrutura, dos requisitos de dados pessoais, bem como da maturidade de compliance da Santa Casa de Paranavaí;
vi. Lançamento e implementação de mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais, sejam tais atividades novas, majoritárias ou com alterações;
vii. Conclusão de um inventário de dados pessoais, destacado no início desta seção, com a lista dos principais processos que utilizam dados pessoais da Santa Casa de Paranavai.
viii. Alcance de credibilidade e valor entre os dirigentes da Santa Casa de Paranavaí;
ix. Apresentação de minuta de política de privacidade aos dirigentes da Santa Casa de Paranavaí, com o comprometimento de revisar, conforme os apontamentos de melhorias sugeridos;
x. Projeção ou refinamento de uma nova estratégia de privacidade: um mapeamento do atual cenário e fornecimento de uma visão geral do orçamento necessário para, no mínimo, os próximos 12 meses, bem como a associação e o relacionamento aos pontos de atenção listados;
xi. Neste início sugere-se concentrar em poucos assuntos, balanceando entre as áreas de maior risco e as mais simples da Santa Casa de Paranavaí, quanto a privacidade dos dados. Por exemplo, alternar entre o projeto com maior risco, no que envolve dados pessoais, e uma campanha de sensibilização para os colaboradores.

2.1.2 - Alinhamento de Expectativas com a Alta Administração

Ao longo da etapa de Iniciação e Planejamento é importante ainda alinhar as expectativas com a alta administração, priorizando as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvidas.

Utilizando sua metodologia a DPO Serviços indicou e foi acatada a metodologia que será utilizada para atingir o objetivo de completar o trabalho de adequação da Santa Casa de Paranavaí.

Planejamento de execução

Macro Atividade	2023												2024											
	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho	Agosto	Setembro	Outubro	Novembro	Dezembro	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho	Agosto	Setembro	Outubro	Novembro	Dezembro
Elaborar o Data Mapping																								
Mapear os sistemas, dispositivos de segurança e armazenamento																								
Mapear arquivos físicos com dados de titulares																								
Criar Mapa de Riscos X Impactos X Mitigação																								
Criar Planos de Ação (Processos, Ferramentas e Pessoas)																								
Consolidar dos Fluxos de dados - Base para o Data Mapping - Visão de processo de negócios (Titulares)																								
Rever Processos (Impacto LGPD)																								
Elaboração do RIPD - Relatório Impacto a proteção de Dados																								
Ajustar Processos (Impacto LGPD)																								
Analisar Sistemas (Impacto LGPD)																								
Ajustar em Sistemas (Melhores Práticas)																								
Mapear Integrações (softwares de terceiros internos e operadores)																								
Ajustar os sistemas, dispositivos de segurança e armazenamento																								
Treinamento e Conscientização (Indui Campanha e cartazes em lugares estratégicos)																								
Definir que níveis de segurança e controles devem ser utilizados																								
Criar o plano de Due Diligence para operadores de dados (Descobrir, ver gaps, formalizar)																								
Propor de Redução de Coleta e ciclo de vida de dados																								
Propor Anonimização (se aplicavel) para dados sensiveis																								
Auditorias com colaboradores por amostra																								
Elaborar documentos e manter versão (Termos, Politicas, Contratos)																								
Elaborar Plano de Atendimento a Titulares																								
Elaborar Plano de Resposta a Incidentes																								

2.1.3 – Maturidade da Organização

Outro ponto a se analisar é a maturidade da organização, observando fatores como a rastreabilidade de dados - estruturando-os e descrevendo as informações tratadas em cada sistema -, a comunicação com o paciente e a transparência (elaborando, por exemplo, a política de privacidade e termos de uso de serviços).

2.1.4 – Medidas de Segurança

Na etapa de Iniciação e Planejamento, medidas de segurança também devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas. Nesse cenário, uma das ferramentas que podem auxiliar na construção do PROJETO DE ADEQUAÇÃO como um todo é o Guia de Boas Práticas da LGPD que foi criado originalmente para fornecer orientações de boas práticas aos órgãos e entidades da Assistência a saúde Federal direta.

Já foi dado andamento como suporte para a estrutura do PROJETO DE ADEQUAÇÃO, assim como para a realização das atividades do encarregado provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD o estabelecimento do canal do titular.

2.1.6 – Inventário de Dados Pessoais

Para obter um mapeamento dos dados pessoais utilizados pela Santa Casa de Paranavai, será realizado o inventário de dados, especialmente dos dados pessoais. Conforme o representa documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD. O inventário consiste em uma excelente forma de fazer um balanço do que a Santa Casa de Paranavai faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

Conforme estabelecido em contrato foi apresentado o cronograma abaixo de trabalho visando atingir o objetivo de mapear todos os processos que tratam dados pessoais dentro da Santa Casa de Paranavaí.

Área para Mapeamento (Reunião 1 hora por área)	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho	Agosto	Setembro	Outubro	Novembro	Dezembro
Enfermagem (B, C, D, E), Pediatria e Maternidade, Maternidade, Berçário												
Pronto Socorro, Ambulatório, Ortopedia												
UTI (Adulto, Neo/Pediátrica), Centro Cirúrgico e Obstétrico, Centro de Esterilização												
CCIH, Psicologia, Serviço Social, N. Seg. Paciente, Nutrição e Dietética, Fisioterapia												
SPP (Guarita, Recepção, PABX, SACE), Central de Abastecimento/Almoxarifado												
Compras/Suprimentos, Materiais especiais (Consignados), Farmácia												
Laboratório/Posto de Coleta												
SESMT - Segurança												
Faturamento												
Contabilidade, Tesouraria, Auditoria												
SAME												
Tecnologia da Informação												
Comunicação e Marketing												
Ouvidoria, Controladoria												
Recursos Humanos												
Pedagogia, Educação Continuada, Escolinha												
Enquadramento BL e Riscos												
Apresentação DM												
Revisão de Processos												
Ajustes TI												
Ajustes SAME												
Avaliação projeto												
Planejamento nova onda												

2.1.7 – Levantamento de Contratos relacionados a Dados Pessoais

O levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

Também preliminarmente já foram analisados e apontados diversos riscos em contratos existentes para que sejam já de antemão corrigidos.

Para a máxima clareza, elabore cláusulas específicas conforme as exigências da LGPD, como:

O compartilhamento de dados sensíveis entre empregador e empregado, situação que exige maior cuidado em relação à proteção de dados e que traz disposições específicas na LGPD, como as tratadas no art. 11 da lei.

a) Especifique como a empresa faz a coleta e o tratamento de dados;
b) Deixe claro a possibilidade de o titular acessar os seus dados coletados;
c) Procedimentos para correção, bloqueio ou eliminação de dados mediante solicitação do titular;
d) Informe sobre a possibilidade de revogação do consentimento;
e) Especifique quem tem acesso aos dados e o responsável por seu uso e tratamento;
f) Informe sobre as medidas de proteção e segurança dos dados coletados e armazenados pela empresa.

DPO SERVIÇOS

SANTACASA DE PARANAVAI

Para a máxima clareza, elabore cláusulas específicas conforme as exigências da LGPD, como:

g) Inclusão de Cláusulas Contratuais Preventivas- constar a política da empresa em caso de vazamento de dados (SEMPRE SEGUINDO O PROJETO DE ADEQUAÇÃO DA LGPD);

h) Algumas dessas cláusulas devem conter: a separação de responsabilidades entre as partes do contrato, com a disposição de métodos de auditoria e até mesmo possíveis sanções e punições no caso do desrespeito à legislação, ou ainda, Cláusulas que tratem de padrões e exigências mínimas de segurança da informação, bem como a possibilidade de transferência internacional de dados deve estar prevista e protegida além da transferência de dados pessoais em território brasileiro também precisa estar bem definida em cláusulas específicas;

i) Em outros casos, é importante que o contrato deixe claro para todas as partes as práticas de Compliance e proteção de dados tomadas internamente na empresa, como a política interna de privacidade, códigos de ética e segurança da informação, entre outros, exigindo de todas as partes dos contratos que se comprometam a manter o nível de proteção de dados previsto.

Contrato de Trabalho a Título de Experiência

DANILO INACIO BORGES

SUGESTÇÃO DE ADEQUAÇÃO
Separação do Contrato em Clausulas, parágrafos, alíneas e incisos e Descrição do Objeto e a função no Objeto contratual;
Estabelecer com clareza a remuneração e a forma de remuneração contendo seus possíveis reajustes, bonificações e descontos;
Estabelecer a forma do registro de horários de trabalho;
Regulamentar a redação do compromisso com as regas de compliance (Regimento Interno);
Incluir o recebimento do documento da política de privacidade de dados;
Estabelecer responsabilização pessoal sob a infringência dos dados que tiver acesso; Cláusulas de finalidade legítima;
Cláusula sobre a possibilidade da revogação do consentimento e sobre os resultados desta decisão no contexto do contrato;
Cláusula sobre os procedimentos para a correção, bloqueio ou eliminação de dados (retificação);

PRESTAÇÃO DE SERVIÇOS DO TICKET ALIMENTAÇÃO

TICKET

SUGESTÇÃO DE ADEQUAÇÃO
Tentar renegociar os parâmetros de penalidade por inadimplementos (TENTAR PELO MENOS ALGO FLEXÍVEL);
Cláusula de Comunicação de incidentes;
Cláusula sobre os procedimentos para a correção, bloqueio ou eliminação de dados (retificação);
Regulamentar a redação do compromisso com as regas de compliance (Regimento Interno);
Incluir o recebimento do documento da política de privacidade de dados;
Cláusula sobre como a empresa coleta os dados e quais dados são coletados;
Cláusula sobre a possibilidade da revogação do consentimento e sobre os resultados desta decisão no contexto do contrato;
Cláusula sobre o procedimento para que o titular exerça seu direito de acesso aos dados coletados

CONTRATO DE PARCERIA NA REALIZAÇÃO DE EXAMES DE ECO

DOPPLER – CARDIÓGRAFO

SUGESTÇÃO DE ADEQUAÇÃO
Descrever as exceções no parágrafo único da Clausula 1ª; Clausula 2ª bem genérica, verificar necessidade de especificação
Clausula 3ª – verificar o fato gerador se está correto na prática do dia -a-dia; Cláusula 4º - quais tipos de riscos, especificar os mais comuns e similares;
Na cláusula quinta necessário estar constando o procedimento a ser adotado quando for acordado a alterado da forma de prestação de serviço; Na cláusula sexta incluir ao final no texto sob pena de ...
Na Cláusula sétima está de maneira genérica o fornecimento dos materiais a serem utilizados AA necessidade da especificação desses materiais;
Cláusula nona necessidade de alteração quanto ao prazo de duração do contrato, sob pena de ficaram muito exposto;
Na cláusula 11ª deverá ser incluído o controle de registro dos residentes que farão uso dos equipamentos no estágio;
Adequar clausulas para garantir mais segurança no tratamento de dados pessoais;
Incluir cláusulas de proteção e privacidade de dados quando acessado ou quando qualquer dos responsáveis tiver acesso a dados .
A cláusula deve ser escrita, clara e transparente, informando sobre o uso que será feito de qualquer dos dados em que as part es tiverem acesso, contendo ainda para qual finalidade e qual procedimento a empresa adotará no uso desses dados (adequação ao fluxo trabalhado no planejamento)

CONTRATO DE SERVIÇOS HOSPITALERES

PARANÁ ASSISTÊNCIA

SUGESTÇÃO DE ADEQUAÇÃO
Incluir cláusulas de proteção e privacidade de dados quando acessado ou quando qualquer dos responsáveis tiver acesso a dados . Adequar clausulas para garantir mais segurança no tratamento de dados pessoais;
Cláusula de Comunicação de incidentes;
Cláusula sobre os procedimentos para a correção, bloqueio ou eliminação de dados (retificação);
A cláusula deve ser escrita, clara e transparente, informando sobre o uso que será feito de qualquer dos dados em que as part es tiverem acesso, contendo ainda para qual finalidade e qual procedimento a empresa adotará no uso desses dados (adequação ao fluxo trabalhado no planejamento)
Incluir o recebimento do documento da política de privacidade de dados;
Cláusula sobre como a empresa coleta os dados e quais dados são coletados;
Cláusula sobre a possibilidade da revogação do consentimento e sobre os resultados desta decisão no contexto do contrato;

CONTRATO DE PRESTAÇÃO DE SERVIÇOS

HANNA BET EIRELI

SUGESTÇÃO DE ADEQUAÇÃO
Adequação do contrato em formato ABNT – clausulas e parágrafos;
No objeto contratual trazer clareza quanto a terceirização e quarteirização de contratação; Incluir cláusulas de proteção e privacidade de dados quando acessado ou quando qualquer dos responsáveis tiver acesso a dados .
Adequar clausulas para garantir mais segurança no tratamento de dados pessoais;
A cláusula deve ser escrita, clara e transparente, informando sobre o uso que será feito de qualquer dos dados em que as part es tiverem acesso, contendo ainda para qual finalidade e qual procedimento a empresa adotará no uso desses dados (adequação ao fluxo trabalhado no planejamento)
Incluir o recebimento do documento da política de privacidade de dados;
Cláusula sobre como a empresa coleta os dados e quais dados são coletados;
Cláusula sobre a possibilidade da revogação do consentimento e sobre os resultados desta decisão no contexto do contrato;
Responsabilização do uso dos dados;
Cláusula sobre o procedimento para que o titular exerça seu direito de acesso aos dados coletados

CONTRATO DE PRESTAÇÃO DE SERVIÇOS

CINPETI CLÍNICA MÉDICA - NEUROCIRURGIA

SUGESTÇÃO DE ADEQUAÇÃO
Adequação do contrato em formato ABNT – clausulas e parágrafos;
No objeto contratual trazer clareza quanto a terceirização e quarteirização de contratação; Incluir cláusulas de proteção e privacidade de dados quando acessado ou quando qualquer dos responsáveis tiver acesso a dados .
Adequar clausulas para garantir mais segurança no tratamento de dados pessoais;
A cláusula deve ser escrita, clara e transparente, informando sobre o uso que será feito de qualquer dos dados em que as part es tiverem acesso, contendo ainda para qual finalidade e qual procedimento a empresa adotará no uso desses dados (adequação ao fluxo trabalhado no planejamento)
Incluir o recebimento do documento da política de privacidade de dados;
Cláusula sobre como a empresa coleta os dados e quais dados são coletados;
Cláusula sobre a possibilidade da revogação do consentimento e sobre os resultados desta decisão no contexto do contrato;
Responsabilização do uso dos dados;
Cláusula sobre o procedimento para que o titular exerça seu direito de acesso aos dados coletados

2.2 – Construção e Execução

Além do texto apresentado na LGPD, pode-se inferir da ABNT ISO/TR 18638:2019 que, considerando os departamentos da Santa Casa de Paranavai, um PROJETO DE ADEQUAÇÃO deve ser projetado para proteger os direitos do paciente em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes.

Assim, na etapa de construção de um programa de gerenciamento da privacidade, deve-se considerar os direitos do titular, a limitação e rastreabilidade dos acessos a dados e a redução do risco de exposição através de medidas técnicas tais como segurança em TI.

2.2.1 – Políticas e práticas para proteção da privacidade do paciente da Santa Casa de Paranavai

Na construção de um PROJETO DE ADEQUAÇÃO devem ser especificadas políticas e práticas para proteger a privacidade do paciente da Santa Casa de Paranavai, garantindo que todos os usos dos dados pessoais são conhecidos e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada. Além das políticas e práticas, na Assistência a saúde, papéis específicos dos colaboradores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais devem ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos pacientes da Santa Casa de Paranavai em relação aos seus direitos quanto à privacidade da informação.

Informações como a finalidade da Santa Casa de Paranavaí e a base legal para tratamento de dados, obtidas no inventário dos dados pessoais, realizado na fase de Iniciação e Planejamento, são úteis na construção das operações de tratamento. Tais informações auxiliam na determinação dos detalhes do ciclo de vida dos dados pessoais, por exemplo a finalidade do tratamento, como, onde e por quanto tempo é o armazenamento, entre outros.

2.2.2 – Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

É ainda na etapa de Construção e Execução do PROJETO DE ADEQUAÇÃO que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

2.2.3 – Medidas e Política de Segurança da Informação e Política de Privacidade

Ainda na etapa de Construção e Execução do PROJETO DE ADEQUAÇÃO, tem-se o desenvolvimento e/ou a atualização das diretrizes internas de proteção de dados pessoais. Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário revisar contratos. Desse modo, torna-se fundamental o desenvolvimento de uma política de segurança da instituição.

Também é necessário a elaboração de uma Política de Privacidade. A Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário. A Política de Privacidade, que faz parte do Termo de Uso, origina se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6º LGPD. Portanto, o documento é, ao mesmo tempo, um dever do controlador e um direito do titular. Assim deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente e como os princípios abaixo são atendidos.

i. Finalidade: Obrigatoriedade de tratamento somente para fins legítimos, específicos, explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I);

ii. Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II);

iii. Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (art. 6º, III);

iv. Livre acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV).

v. Qualidade dos dados: Critérios de qualidade dos dados, para garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V).

vi. Transparência: Critérios de transparência, para garantir, aos titulares, o fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI). Segurança: Critérios de segurança, para que se utilize medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII);

vii. Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII);

viii. Não discriminação: Critérios de não discriminação, para garantir que não se realize o tratamento de dados para fins discriminatórios ilícitos ou abusivos (art. 6º, IX).

ix. Responsabilização e prestação de contas: para que, para cada tratamento de dados se possa demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º, X).

A Política de Privacidade da Santa Casa de Paranavai conterá, no mínimo seguintes tópicos:

i. Controlador
ii. Operador
iii. Encarregado
iv. Quais dados são tratados
v. Como os dados são coletados
vi. Qual o tratamento realizado e para qual finalidade
vii. Compartilhamento de dados
viii. Segurança dos dados
ix. Tratamento posterior dos dados para outras finalidades

As medidas de segurança para a proteção dos dados pessoais devem ser implementadas na fase de Construção do Plano Diretor de Privacidade (PDP).

Por fim, mas não menos importante, os direitos dos titulares precisam ser gerenciados. Devem ser destacadas e elucidadas questões como a diferença entre o titular e o custodiante do dado pessoal, do ponto de vista da Assistência a saúde, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade.

2.2.4 – Adequação Cláusulas Contratuais

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento, é importante rever os documentos vigentes e os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que a Assistência a saúde revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame.

Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD, apresentados em seu art. 6º. Como um dos princípios listados é a transparência, torna-se essencial que o contrato apresente informações claras e objetivas, abordando, se pertinente:

i. Delimitações claras e objetivas das responsabilidades do controlador e operador;
ii. A forma que é realizada a coleta e o tratamento de dados;
iii. A existência da possibilidade de o titular acessar os seus dados coletados;
iv. A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
v. A existência da possibilidade de revogação do consentimento dado pelo titular;
vi. O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
vii. As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

2.2.5 – Termo de Uso

Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele.

O Termo de Uso, como a Política de Privacidade, advém da consciência do controlador e operador ser transparente com o titular de dados pessoais e comunicar como as atividades de tratamento desses dados observam os princípios dispostos no artigo 6º da LGPD. Em cumprimento aos princípios da publicidade e da transparência, e a fim de assegurar aos pacientes da Santa Casa de Paranavai amplo acesso às informações, os termos devem ser regularmente atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados pela Santa Casa de Paranavai e entidade no exercício de suas competências legais ou execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Os tópicos que devem constar no Termo de Uso estão listados no quadro a seguir:

i. Aceitação dos Termos e Políticas
ii. Definições
iii. Arcabouço Legal
iv. Descrição do serviço
v. Direitos do usuário
vi. Responsabilidades do usuário e da Assistência a saúde na Santa Casa de Paranavai
vii. Mudanças no Termo de Uso
viii. Informações para contato
ix. Foro

2.2.6 – O Encarregado

Na etapa de Construção/Execução, realizará as seguintes atividades:

i. Implementação das ações identificadas na fase de Iniciação e Planejamento;
ii. Demonstração, para os dirigentes da Santa Casa de Paranavaí, do progresso e dos resultados obtidos com as atividades envolvendo o inventário dos dados e a divulgação e conscientização da LGPD junto aos colaboradores.
iii. Se necessário, redefinição de prioridades, baseando-se nos resultados alcançados e no retorno dos dirigentes e gestores da Santa Casa de Paranavaí.
iv. Estabelecimento e manutenção de documentação relacionada à LGPD e aos dados pessoais tratados na Santa Casa de Paranavai, com informações sobre: atividades em andamento e planejadas; responsáveis pelos serviços e sistemas que utilizam dados pessoais; e incidentes e vazamento de dados pessoais.
v. Definição de mecanismos de reportes internos, assegurando transparência e rapidez na troca de informação, além de reafirmar o papel como facilitador, suporte e nunca um obstáculo.

2.3 – Monitoramento

Acompanhar a conformidade à LGPD é uma atividade contínua e necessária para manter o PROJETO DE ADEQUAÇÃO a longo prazo. Assim sendo, esta última etapa do PROJETO DE ADEQUAÇÃO aborda aspectos, detalhados nas próximas seções, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados.

2.3.1 – Indicadores de Performance

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Programa de Governança em Privacidade assim como o status de outras iniciativas de privacidade.

Recomenda-se o uso dos seguintes indicadores:

i. Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
ii. Resultados do Diagnóstico de Adequação à LGPD - índice de adequação;
iii. Índice de processos com dados pessoais inventariados: número de processos com dados pessoais inventariados / número de processo com dados pessoais da Santa Casa de Paranavai * 100;
iv. Índice de processos com RIPD elaborado: quantidade de processos com RIPD elaborado / quantidade de processos da Santa Casa de Paranavaí * 100;
v. Índice de conscientização em segurança: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100;
vi. Índice de quantidade de controles de segurança e privacidade implementados para um determinado processo: quantidade de controles de segurança e privacidade implementados para um determinado processo / quantidade total de controles de segurança e privacidade identificados para o processo * 100.

2.3.2 – Gestão de Incidentes

É importante incluir nesta etapa do PROJETO DE ADEQUAÇÃO um processo de Gestão de Incidentes, que registre os incidentes de segurança da informação e de privacidade ocorridos e que armazene informações como: a descrição dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências.

É válido também implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual a Solução de TIC e/ou a Santa Casa de Paranavai estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela Santa Casa de Paranavai.

É recomendado ainda que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

2.3.3 – Análise e Reporte de Resultados

A análise e o reporte de resultados também é indicado na etapa de monitoramento para demonstrar o valor do PROJETO DE ADEQUAÇÃO para a alta administração. Mostrar a evolução das ações e resultados obtidos, bem como o papel da privacidade para o paciente reforçam e fortalecem a cultura de privacidade dos dados.

2.3.4 – O Encarregado

O encarregado, dado seu papel de articulação, exerce função fundamental nessa etapa:, conforme apontado no quadro a seguir.

i. Gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do Plano Diretor de Privacidade (PDP);

ii. Divulgação dos resultados entre as diversas áreas da Santa Casa de Paranavaí – estabelecimento de uma estrutura de divulgação de resultados para a diretoria da Santa Casa de Paranavai.

A incorporação, em um PROJETO DE ADEQUAÇÃO, destes passos ajudará a garantir que o programa abordará os regulamentos de privacidade de dados e ajudará a criar e conquistar a confiança do paciente titular dos dados por meio da demonstração do cuidado com seus dados pessoais e sua privacidade.

Referências Bibliográficas

- GUIA LGPD PARA O SETOR HOSPITALAR – FBH – Federação Brasileira de Hospitais - https://www.fbh.com.br/wp-content/uploads/2021/02/Guia-LGPD.pdf
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação.
- ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.
- ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/TR 18638:2019- Informática em saúde — Orientações sobre educação da privacidade das informações em saúde em organizações de assistência à saúde.
- ARTICLE 29 DATA PROTECTION WORKING PARTY. WP29 guidelines on the Data Protection Officer requirement in the GDPR. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 Acesso em: 19 ago. 2020.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 20 ago. 2020.
- Cavoukian, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009. Disponível em: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf. Acesso em: 13 jan. 2020.
- GARTNER GROUP. The Privacy Officer's First 100 Days. 2018. Disponível em: https://www.gartner.com/en. Acesso em: 21 ago. 2020.
- KORFF, Douwe; GEORGES, Marie. The DPO Handbook: Guidance for data protection officers in the public and quase-public sectors on how to ensure compliance with the european union general data protection regulation. Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation. 2019. Disponível em: https://ssrn.com/abstract=3428957. Acesso em: 20 ago. 2020.
- PROJECT MANAGEMENT INSTITUTE. Um Guia de Conhecimento em Gerenciamento de Projetos. Guia PMBOK 5a edição. Project Management Institute, 2013.