1) Dados a serem coletados — lista e classificação

Para cada item: (Dado) — Classificação: Pessoal Comum / Pessoal Sensível

1. *Nome completo — Pessoal Comum*
2. *CPF — Pessoal Sensível (identificador)*
3. *RG (opcional) — Pessoal Sensível*
4. *Data de nascimento — Pessoal Comum*
5. *Sexo — Pessoal Comum*
6. *Telefone(s) — Pessoal Sensível*
7. *E-mail — Pessoal Comum*
8. *Endereço (rua, número, cidade, CEP) — Pessoal Sensível*
9. *Conveniado (plano de saúde: nome, número da carteirinha) — Pessoal Comum / dados contratuais*
10. *Histórico clínico (diagnósticos, evolução, prescrições, laudos) — Pessoal Sensível (dados de saúde).*
11. *Registro de sessões/atendimentos (data, fisioterapeuta, tipo de sessão, observações clínicas) — Pessoal Sensível (quando contém info de saúde).*
12. *Alergias e medicações em uso — Pessoal Sensível (saúde).*
13. *Fotografias / imagens (ex.: evolução de postura, exames) — Pessoal Sensível (pode revelar condição de saúde / biometria).*
14. *Logs de acesso ao prontuário (quem acessou, quando) — Pessoal Comum (registro de tratamento)*

2) Finalidade e Base Legal (resumo por dado essencial)

- *Nome, CPF, telefone, e-mail, endereço*
    - *Finalidade: identificar o titular, contatar para agendamentos, faturamento e envio de documentos.*
    - *Base legal: Execução de contrato (Art. 7º, V) — quando o paciente contrata serviços; cumprimento de obrigação legal (Art. 7º, II) para notas fiscais/obrig. tributárias. (Também pode haver consentimento para comunicações de marketing).*
- *Data de nascimento / sexo*
    - *Finalidade: cálculo de limites de exercícioss, ajuste de condutas clínicas, identificação.*
    - *Base legal: Execução de contrato / Legítimo interesse (quando necessário para segurança e cuidado clínico) — preferir justificar clinicamente.*
- *Dados de pagamento*
    - *Finalidade: cobrança e prova de pagamento.*
    - *Base legal: Execução de contrato e cumprimento de obrigação legal.*

- *Dados de saúde (histórico clínico, diagnósticos, alergias, imagens, prescrições)*
    - *Finalidade: prestar atendimento de fisioterapia com segurança e eficácia; elaborar plano terapêutico; encaminhamentos.*
    - *Base legal: Tutela da saúde / execução de contrato e consentimento explícito quando o dado sensível não for estritamente necessário. A LGPD exige hipóteses específicas para tratamento de dados sensíveis (Art. 11). Em ambientes de saúde, o tratamento para prestação de serviços de saúde costuma se enquadrar como necessário à tutela da saúde, mas sempre com medidas especiais de proteção e, quando possível, consentimento explícito.*
- *Fotografias / imagens clínicas / biometria*
    - *Finalidade: documentação da evolução clínica; autenticação (se biométrica).*
    - *Base legal: Consentimento explícito (para imagens) ou hipótese de tutela da saúde se for estritamente necessário ao tratamento; Art. 11 para sensíveis.*
- *Logs de acesso e auditoria*
    - *Finalidade: segurança, accountability, investigação de incidentes.*
    - *Base legal: Legítimo interesse do controlador e cumprimento de obrigação legal/segurança. (Tratar com cuidado e retenção mínima.)*

3) Princípio da Necessidade — dados excessivos e alternativas de minimização

Excessivos / questionáveis:

- Data de aniversário completa: se o sistema precisa apenas checar idade (maior de 18), armazenar ano de nascimento basta.
- RG: redundante se CPF já é coletado; pode ser opcional.
- Fotografias faciais para finalidades administrativas (ex.: cartão de identificação) — evitar se não essencial.
- Biometria para login — evitar se houver alternativas (2FA via app, OTP).
- Endereço completo quando só se precisa de cidade/CEP para encaminhamento ou faturamento — armazenar apenas o mínimo necessário.

Minimização / anonimização propostas:

- Pseudonimização: separar identificadores diretos (nome, CPF) em tabela distinta e usar um identificador interno (patient_id) no histórico clínico.

- Anonimização para pesquisas: após retenção legal (ex.: 5 anos), anonimizar o CPF e nome em registros usados para pesquisa estatística; manter apenas dados agregados.
- Dados de pagamento: armazenar token do provedor de pagamento em vez do número completo do cartão; guardar apenas os últimos 4 dígitos e data de validade se necessário.
- Retenção mínima: manter prontuário ativo pelo período legal/regulatório aplicável e mover para arquivo criptografado ou anonimizado após esse prazo.