REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

CERTIFICAÇÃO DIGITAL E GOVERNANÇA DA CONFIANÇA NO SUS: SEGURANÇA, INTEROPERABILIDADE E EQUIDADE NA SAÚDE DIGITAL

DIGITAL CERTIFICATION AND TRUST GOVERNANCE IN BRAZIL'S UNIFIED HEALTH SYSTEM: SECURITY, INTEROPERABILITY AND EQUITY IN DIGITAL HEALTH

Ciências Sociais Aplicadas • 22/11/2026

REGISTRO DOI: 10.70773/revistatopicos/795168670

Jorge Fernando Prates Ribeiro[1]

Leonardo de Souza Moldero[2]

Moisés Figueiredo da Silva[3]

Luís Fernando Massonetto[4]

Antônio Pires Barbosa[5]

RESUMO

Objetivo: analisar criticamente a contribuição dos certificados digitais e das assinaturas eletrônicas para a confiança institucional, a proteção dos dados e a interoperabilidade do Sistema Único de Saúde (SUS), identificando condições de implementação compatíveis com a equidade e a governança interfederativa. Método: estudo qualitativo, exploratório e propositivo, desenvolvido mediante revisão narrativa crítica de literatura científica selecionada e análise documental de normas e documentos institucionais, com ênfase no período 2018–2026. Foram examinadas a legislação brasileira de identidade e proteção de dados, a documentação técnica da Rede Nacional de Dados em Saúde (RNDS), diretrizes internacionais e estudos empíricos sobre prontuários e integração de dados no SUS. Resultados: a literatura e a documentação confirmam que certificados da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) integram mecanismos de autenticação e de assinatura qualificada, inclusive nas conexões institucionais com a RNDS; entretanto, não substituem regras de autorização, padrões semânticos, segurança operacional ou governança de dados. Estudos nacionais documentam a ampliação da informatização da atenção primária e experiências de interoperabilidade entre redes, sem permitir atribuir tais avanços exclusivamente à certificação digital. Propõe-se uma matriz de governança da confiança digital com dimensões técnico-jurídicas, assistenciais, organizacionais e distributivas, acompanhada de indicadores de avaliação. Conclusão: a certificação digital constitui infraestrutura habilitadora relevante, mas sua contribuição para o SUS depende de integração com interoperabilidade clínica, proteção de dados, competências institucionais e mecanismos inclusivos de acesso.

Palavras-chave: Certificação digital; Saúde digital; Sistema Único de Saúde; Interoperabilidade; Governança de dados; Equidade.

ABSTRACT

Objective: to critically examine how digital certificates and electronic signatures contribute to institutional trust, data protection, and interoperability within Brazil's Unified Health System (SUS), identifying implementation conditions consistent with equity and intergovernmental governance. Methods: a qualitative, exploratory, and proposal-oriented study combining a critical narrative review of selected scientific literature with documentary analysis of legal and institutional sources, primarily covering 2018–2026. Brazilian rules on digital identity and data protection, technical documentation on the National Health Data Network (RNDS), international guidance, and empirical research on electronic records and health information exchange were assessed. Results: the evidence supports the role of certificates issued under Brazil's Public Key Infrastructure (ICP-Brasil) in authentication and qualified signatures, including institutional connections to the RNDS. However, certificates alone do not ensure authorization, semantic interoperability, operational security, or data governance. Brazilian studies describe the expansion of primary-care digital records and practical data exchange initiatives, but these developments cannot be causally attributed to digital certification. The study proposes a digital trust governance matrix integrating legal-technical, clinical, organizational, and distributive dimensions, supported by assessment indicators. Conclusion: digital certification is an important enabling infrastructure, yet its contribution to public health depends on integration with clinical interoperability, personal data protection, institutional capabilities, and inclusive access mechanisms.

Keywords: Digital certification; Digital health; Unified Health System; Interoperability; Data governance; Equity.

1. INTRODUÇÃO

A transformação digital dos sistemas de saúde é frequentemente apresentada como solução para fragmentação informacional, descontinuidade assistencial e ineficiência administrativa. Entretanto, digitalizar documentos e ampliar canais eletrônicos não equivale, necessariamente, a produzir integração clínica, segurança informacional ou inclusão. A Organização Mundial da Saúde (OMS, 2025) destaca que estratégias digitais efetivas dependem da articulação de recursos tecnológicos, humanos, financeiros e institucionais. No Brasil, Haddad e Lima (2024) situam a saúde digital como agenda de política pública, vinculada ao fortalecimento do Sistema Único de Saúde (SUS) e ao direito à saúde.

A dimensão territorial brasileira impõe desafios adicionais. Municípios apresentam capacidades fiscais, administrativas e tecnológicas distintas; profissionais transitam entre unidades e níveis de atenção; usuários demandam continuidade de registros ao longo do cuidado. A pesquisa de Silva (2023), referente ao planejamento de serviços de saúde em Ilhabela/SP, e o artigo de Silva, Trindade e Barbosa (2023) evidenciam a relevância de indicadores e informações confiáveis para decisões de gestão na escala municipal. Essas produções fundamentam o vínculo entre qualidade dos dados, capacidade estatal e planejamento, mas não constituem avaliações empíricas do efeito de certificados digitais.

O atual ambiente normativo incorpora a Estratégia de Saúde Digital para o Brasil 2020–2028, o Programa SUS Digital e a Rede Nacional de Dados em Saúde (RNDS), cuja governança foi disciplinada pelo Decreto nº 12.560/2025. Em julho de 2026, o Ministério da Saúde divulgou a continuidade da federalização da RNDS e o início de sua etapa de municipalização, reforçando a importância de soluções

coordenadas entre União, estados e municípios (BRASIL, 2020; BRASIL, 2024; BRASIL, 2025; Ministério da Saúde, 2026).

Nesse contexto, certificados digitais são instrumentos de identificação vinculados a chaves criptográficas, capazes de apoiar a autenticação e, quando utilizados para assinatura, a verificação de autoria e integridade. A RNDS prevê sua utilização em processos de credenciamento e autenticação institucional, inclusive por certificados ICP-Brasil associados ao estabelecimento ou ao respectivo gestor (MINISTÉRIO DA SAÚDE, s.d.-a). Todavia, tal vínculo não substitui políticas de acesso clínico, interoperabilidade de dados nem as obrigações previstas na Lei Geral de Proteção de Dados Pessoais (LGPD).

A questão central desta pesquisa é: sob quais condições técnicas, jurídicas, administrativas e sociais a certificação digital pode fortalecer a confiança no intercâmbio de informações do SUS, sem criar novas barreiras de acesso ou falsas garantias de segurança? O objetivo geral consiste em analisar essas condições de implementação e propor um referencial de governança aplicável às diferentes esferas do SUS. Especificamente, busca-se: diferenciar mecanismos de identidade e assinatura; examinar a arquitetura institucional e regulatória brasileira; confrontar promessas tecnológicas com evidências disponíveis; e construir dimensões e indicadores para avaliação futura.

A contribuição do artigo está em deslocar o debate da adoção isolada de uma tecnologia para o desenho de uma infraestrutura pública de confiança. Em perspectiva jurídico-institucional, a crítica de Massonetto, Bachur e Carvalho (2020) à reificação da experiência nas cidades inteligentes adverte contra a conversão do cidadão em

objeto passivo da racionalização tecnológica. Na saúde pública, esse alerta exige que a confiança digital seja aferida também por transparência, controle social, capacidade de contestação e preservação de alternativas acessíveis. A produção recente de Moldero et al. (2026) sobre cuidado oportuno e direitos dos pacientes complementa esse argumento ao relacionar a legitimidade da regulação à possibilidade de verificar critérios, tempos e efeitos concretos sobre o acesso. A discussão converge com as pesquisas recentes de Silva, Trindade e Barbosa (2026) sobre inteligência artificial na gestão da saúde, nas quais a qualidade, a disponibilidade e a proteção das informações constituem pré-condições para aplicações digitais responsáveis. Não se pressupõe, entretanto, que a simples implantação de certificados resulte automaticamente em redução de fraudes, melhora assistencial ou economia orçamentária.

2. PROCEDIMENTOS METODOLÓGICOS

Trata-se de pesquisa qualitativa, de natureza aplicada e finalidade exploratório-analítica, desenvolvida por meio de revisão narrativa crítica da literatura e análise documental de fontes normativas e técnico-institucionais. A escolha dessa classificação decorre do objeto interdisciplinar, que envolve direito, gestão pública, segurança da informação e informática em saúde. Diferentemente de uma revisão sistemática, o estudo não apresenta protocolo previamente registrado, varredura exaustiva de bases, dupla triagem independente nem metanálise. Por essa razão, não se atribui à seleção documental pretensão de completude ou capacidade de estimar efeitos causais.

A seleção intencional do corpus considerou aderência ao tema, rastreabilidade editorial, atualidade normativa e capacidade explicativa. Foram consultados portais oficiais de legislação, Ministério da Saúde/DATASUS, Instituto Nacional de Tecnologia da Informação (ITI), Autoridade Nacional de Proteção de Dados (ANPD), OMS, National Institute of Standards and Technology (NIST), repositório da UNINOVE e publicações indexadas ou acessíveis nos portais SciELO, PubMed e editoras científicas. O período de referência principal foi 2018–2026, admitindo-se normas anteriores indispensáveis, como a Lei nº 8.080/1990 e a Medida Provisória nº 2.200-2/2001. O levantamento e a verificação editorial foram atualizados em 6 de novembro de 2026.

A apreciação das fontes foi organizada em quatro eixos: (a) fundamentos técnicos da identidade, autenticação, assinatura e autorização; (b) normas de proteção de dados e governança interfederativa; (c) interoperabilidade e experiências documentadas no SUS; e (d) equidade, implantação e avaliação. As consultas empregaram termos em português e inglês, entre eles “certificação digital”, “saúde digital”, “RNDS”, “ICP-Brasil”, “health information interoperability”, “electronic health records” e “data governance”. Priorizou-se o documento normativo primário para afirmações sobre obrigações legais, fontes técnico-institucionais para requisitos operacionais e artigos científicos para evidências de implementação, sem converter a existência de diretrizes em prova de efetividade. As fontes foram contrastadas entre si para distinguir obrigações jurídicas, requisitos técnicos, resultados empíricos e recomendações propositivas. O percurso considera o debate metodológico de Silva et al. (2024) quanto à transparência e ao rigor em revisões nas ciências sociais aplicadas, sem caracterizar este trabalho como revisão sistemática efetivamente executada.

Foram excluídas afirmações quantitativas do manuscrito original cuja fonte primária não foi localizada ou cuja obra citada não sustentava o resultado descrito; também se desconsideraram referências incompletas ou sem rastreabilidade confiável. O corpus final priorizou atos normativos vigentes, guias institucionais e estudos com identificação bibliográfica verificável. Como o estudo utiliza exclusivamente informações públicas, não houve coleta primária nem tratamento de prontuários ou dados individuais de pacientes.

As conclusões devem ser lidas de acordo com a hierarquia de evidências empregada. Normas demonstram deveres e condições regulatórias; guias técnicos documentam exigências operacionais; estudos empíricos demonstram resultados em contextos delimitados; e a matriz proposta representa inferência analítica dos autores, a ser testada posteriormente. Essa separação evita converter possibilidades tecnológicas em benefícios já comprovados.

3. REFERENCIAL CONCEITUAL E REGULATÓRIO

3.1. Identidade Digital, Certificação, Autenticação e Assinatura Eletrônica

A certificação digital integra uma infraestrutura de chaves públicas, na qual uma autoridade certificadora vincula determinada identidade a uma chave pública e possibilita validar operações criptográficas correspondentes. Na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), certificados podem identificar pessoas físicas, pessoas jurídicas e, conforme sua finalidade, sistemas e equipamentos (ITI, 2026). A utilidade da certificação depende, entre outros fatores, da verificação de identidade, da

custódia adequada das chaves privadas, da validade temporal, da revogação e da confiança na cadeia certificadora.

É necessário diferenciar quatro operações. Identificação responde a quem se declara ser o sujeito; autenticação verifica credenciais para uma interação; assinatura digital associa um signatário a determinado conteúdo e possibilita detectar modificações; autorização estabelece a quais informações e funções o sujeito autenticado pode ter acesso. A conformidade em uma operação não implica automaticamente conformidade nas demais. As diretrizes de identidade digital NIST SP 800-63-4 distinguem processos de comprovação de identidade, autenticação e federação, reforçando a inadequação de reduzir toda a governança de acesso à posse de um certificado (NIST, 2025).

A Lei nº 14.063/2020 distingue assinaturas eletrônicas simples, avançadas e qualificadas. A assinatura qualificada utiliza certificado ICP-Brasil, mas a legislação também reconhece modalidades adequadas a contextos e níveis de risco determinados. No âmbito da saúde, a classificação da assinatura aplicável deve observar a natureza do documento e a regulamentação específica; não é correto exigir um certificado ICP-Brasil de todo cidadão para qualquer interação com serviço público (BRASIL, 2020b). A própria assinatura avançada Gov.br constitui exemplo de mecanismo juridicamente previsto que não se confunde com assinatura qualificada (ITI, 2024).

Também não se pode confundir assinatura digital com criptografia do armazenamento ou do transporte. Uma assinatura permite verificar a integridade de um documento assinado, mas não o torna necessariamente sigiloso; a proteção de dados em trânsito e em

repouso, a gestão de perfis e a auditoria são medidas complementares. O livro Certificado digital, publicado pela Universidade Federal de Goiás, enfatiza a necessidade de capacitação dos agentes de saúde para a utilização adequada desses recursos (Lucena et al., 2023).

3.2. LGPD, Direitos dos Titulares e Responsabilidade Pública

A LGPD classifica dados referentes à saúde como dados pessoais sensíveis e impõe princípios de finalidade, adequação, necessidade, segurança, prevenção, transparência e responsabilização (BRASIL, 2018). No SUS, o compartilhamento de informações pode decorrer de atribuições legais, execução de políticas públicas e hipóteses específicas de tutela da saúde, de acordo com a operação concreta. Portanto, é juridicamente impreciso afirmar que todo tratamento de informações clínicas depende exclusivamente de consentimento do paciente, assim como é equivocado presumir que a aquisição de certificados digitais satisfaz integralmente a LGPD.

A avaliação de conformidade requer identificar controlador e operadores, finalidade e base legal de cada fluxo, regras de retenção, controle de acesso, registro das operações, resposta a incidentes e garantia dos direitos previstos em lei. O Guia orientativo de tratamento de dados pessoais pelo Poder Público, disponibilizado pela ANPD, oferece parâmetros interpretativos para o uso responsável de dados na administração (ANPD, 2024). A governança digital deve incorporar esses requisitos desde o desenho dos processos e serviços, com especial cuidado para compartilhamentos interinstitucionais e contratação de fornecedores.

Há ainda risco de confusão entre rastreabilidade e vigilância desproporcional. Auditorias são necessárias para apurar acessos, alterações e responsabilidade administrativa; seus registros, porém, devem ser protegidos e acessíveis somente a agentes legitimados. A possibilidade de identificar o operador não legitima consultas indiscriminadas ao histórico clínico. Sob a ótica da equidade, usuários idosos, pessoas com deficiência, populações de baixa conectividade e cidadãos com menor letramento digital demandam canais assistidos e alternativas proporcionais de identificação, para que segurança não signifique exclusão.

3.3. RNDS, Padrões de Dados e Federalismo Sanitário

A Estratégia de Saúde Digital para o Brasil 2020–2028 orienta a consolidação de um ecossistema informacional conectado. A Portaria GM/MS nº 3.232/2024 instituiu o Programa SUS Digital, ampliando o debate para cuidado, vigilância, formação de trabalhadores, planejamento e gestão (BRASIL, 2020a; BRASIL, 2024). O Decreto nº 12.560/2025 disciplinou a RNDS e as Plataformas SUS Digital, enfatizando compartilhamento, interoperabilidade, proteção e governança dos dados de saúde (BRASIL, 2025).

O Guia de Implementação da RNDS especifica o emprego do padrão HL7 FHIR, versão R4, para estruturar a troca de dados entre sistemas. Certificados digitais participam do estabelecimento de relações confiáveis entre sistemas/organizações, ao passo que padrões como FHIR descrevem recursos, mensagens, perfis e significados interoperáveis. Desse modo, certificação e interoperabilidade cumprem funções distintas e complementares: a primeira contribui para reconhecer e proteger interações; a segunda permite que as

informações sejam interpretadas e utilizadas entre aplicações heterogêneas (MINISTÉRIO DA SAÚDE, s.d.-b; HL7, 2019).

A documentação oficial da RNDS informa que certificados ICP-Brasil são empregados no credenciamento e na autenticação de conexões, podendo estar associados ao e-CPF do gestor ou ao e-CNPJ do estabelecimento, conforme o processo de solicitação de acesso. A integração exige requisitos institucionais e técnicos adicionais, como estabelecimento cadastrado, credenciais, homologação e observância dos serviços disponibilizados (MINISTÉRIO DA SAÚDE, s.d.-a; DATASUS, s.d.). Trata-se de autenticação institucional do integrador, e não de prova de que cada registro clínico tenha sido individualmente assinado por profissional de saúde ou autorizado para qualquer consulta.

Na etapa de municipalização anunciada em 2026, o desafio deixa de ser apenas disponibilizar conexões: torna-se necessário compatibilizar capacidades locais, políticas de governança, critérios assistenciais e instrumentos de monitoramento. A gestão municipal precisa distinguir investimento em certificados, interoperabilidade efetiva, melhoria da qualidade dos dados e contribuição para decisões e resultados assistenciais. Essa distinção é consistente com a ênfase de Silva (2023) no uso de informações do SUS para o planejamento público.

4. EVIDÊNCIAS CIENTÍFICAS E ANÁLISE CRÍTICA

4.1. Avanços Documentados na Informatização e na Integração dos Serviços

Os estudos selecionados documentam avanços relevantes na informatização do SUS, embora não estabeleçam um efeito isolado

da certificação digital. Celuppi et al. (2024), com base em registros administrativos da Atenção Primária à Saúde, identificaram que o número de unidades que utilizavam o Prontuário Eletrônico do Cidadão (PEC) passou de 8.930, em 2017, para 26.091, em 2022. O resultado descreve evolução da adesão e do uso de uma solução informacional específica, não uma redução comprovada de fraude ou de incidentes de privacidade. Em diagnóstico de abrangência nacional, o Censo das Unidades Básicas de Saúde de 2024, divulgado pelo Ministério da Saúde em 2025, informou que 94,6% das UBS possuíam acesso à internet e 87% utilizavam prontuário eletrônico. A coexistência dessas taxas com dificuldades de qualidade da conexão ressalta a diferença entre disponibilidade formal de infraestrutura e maturidade operacional (Ministério da Saúde, 2025).

Em outro recorte, Pinto et al. (2025) analisaram experiências de interoperabilidade em Recife e na Empresa Brasileira de Serviços Hospitalares (Ebserh), relatando a integração de plataformas e a federação de dados entre dois ambientes em 2023. Segundo o estudo, a experiência envolveu 45 hospitais da Ebserh e registros de mais de 25 milhões de usuários. O caso demonstra possibilidades de interoperabilidade organizacional e de compartilhamento de informações clínicas, mas não isola o certificado digital como variável explicativa de resultados clínicos e administrativos.

Haddad e Lima (2024) também situam o avanço da saúde digital como processo de reorganização de serviços, no qual informação, telessaúde e políticas públicas de integração se relacionam. Os resultados dialogam com o artigo de Silva, Trindade e Barbosa (2026) sobre inteligência artificial na saúde pública: a potencialidade analítica de sistemas avançados depende de dados completos,

confiáveis e legalmente utilizados. Certificados digitais podem ajudar a consolidar trilhas de responsabilidade e interações institucionalmente autenticadas, mas não corrigem, por si, bases incompletas, codificações incompatíveis ou erros clínicos de origem.

O estudo qualitativo de Orrillo et al. (2025), realizado com 23 gestores estaduais e municipais, identificou benefícios percebidos da informatização para o acesso, a organização do trabalho e a análise de indicadores, mas também dificuldades de infraestrutura, formação de profissionais e dependência de soluções externas. Por outro lado, a revisão integrativa de Gonçalo et al. (2025) identificou desafios operacionais e regulatórios da proteção dos dados de saúde, reforçando que a adequação jurídica não decorre de um único recurso técnico. A convergência entre estudos empíricos e normativos apoia a ideia de um conjunto de condições organizacionais, e não de uma intervenção tecnológica suficiente em si mesma.

A atualização institucional do Ministério da Saúde, em 2026, informou que as 27 unidades da Federação haviam recebido credenciais de acesso à RNDS e que a etapa seguinte priorizaria a municipalização por ciclos. Esse registro constitui evidência documental de expansão organizacional e planejamento de acesso, não prova de que todos os municípios estejam plenamente interoperáveis nem de que a certificação, isoladamente, melhorou indicadores assistenciais (Ministério da Saúde, 2026).

Quadro 1. Evidências verificadas e alcance interpretativo

Fonte	Achado documentado	O que não permite concluir

Celuppi et al. (2024)	PEC e-SUS APS: 8.930 unidades em 2017 e 26.091 em 2022.	Não demonstra efeito causal de certificados na fraude ou na qualidade clínica.
Ministério da Saúde (2025)	94,6% das UBS com internet e 87% com prontuário eletrônico no Censo 2024.	Não mede, por si, a qualidade de conexão ou o efeito da certificação.
Pinto et al. (2025)	Integração Recife–Ebserh; 45 hospitais e registros de mais de 25 milhões de usuários.	Não isola certificação como causa da interoperabilidade.
MS (2026)	Credenciais RNDS nos 27 estados e planejamento de municipalização.	Não equivale à implantação completa em todos os municípios.
DATASUS (s.d.)	Certificado ICP-Brasil requerido para autenticação na RNDS.	Não representa autorização irrestrita ou assinatura individual de cada ato.
Silva (2023)	Indicadores do SUS associados ao planejamento de serviços municipais.	Não mede impactos de PKI em unidades de saúde.

Fonte: elaboração dos autores, com base nos documentos e estudos referenciados (2026).

4.2. Benefícios Possíveis e Limites das Inferências

A certificação digital apresenta uma contribuição tecnicamente delimitada: qualificar a verificação de identidades e de assinaturas, atribuir evidência de integridade a documentos e apoiar a autenticação entre serviços. Em processos com requisitos de assinatura qualificada, a ICP-Brasil agrega mecanismos técnicos e

jurídicos definidos pelo marco brasileiro. Em integração de sistemas, certificados podem fortalecer a confiança nas partes da conexão, desde que sejam corretamente emitidos, armazenados, renovados e revogados (BRASIL, 2001; ITI, 2026; DATASUS, s.d.).

Contudo, há três limites que merecem destaque. Primeiro, autenticidade não significa autorização: credenciais válidas podem ser usadas para finalidades não permitidas se os privilégios forem excessivos ou não houver segregação de funções. Segundo, integridade do documento assinado não significa veracidade clínica: um registro incorreto pode ser assinado corretamente. Terceiro, o emprego de certificado no canal de comunicação não garante padronização semântica: sistemas podem trocar mensagens protegidas e ainda interpretar inadequadamente o significado dos dados.

Assim, expressões como “elimina vulnerabilidades”, “garante confidencialidade” ou “reduz fraudes em determinado percentual” precisam ser substituídas por formulações condicionais, apoiadas no mecanismo efetivamente descrito. Sem desenho de avaliação, grupo comparador ou séries temporais, não é cientificamente defensável atribuir benefícios quantitativos exclusivos à tecnologia. O conjunto de evidências consultado sustenta uma contribuição plausível para a gestão de confiança e não um efeito clínico ou financeiro universal. Essa postura é coerente com a literatura internacional sobre saúde digital, que vincula resultados à maturidade institucional e ao desenho sociotécnico das iniciativas (OMS, 2025).

4.3. Infraestrutura, Custo, Competências e Desigualdade Territorial

A implementação é condicionada por conectividade, equipamentos, disponibilidade dos sistemas, suporte técnico, governança de fornecedores, gestão do ciclo de vida de credenciais e treinamento contínuo. Certificados com chaves privadas exportáveis exigem controles rigorosos de custódia; mecanismos físicos ou gerenciados acrescentam requisitos de suporte e custos. É recomendável que as organizações definam responsáveis, procedimentos para desligamento de profissionais, substituição de gestores, expiração, revogação, contingência operacional e tratamento de incidentes.

O obstáculo distributivo é especialmente relevante em um sistema universal. Municípios com menor capacidade tecnológica podem ser colocados em desvantagem caso a integração dependa de investimentos e competências não acompanhados de apoio interfederativo. A OMS (2025) identifica a equidade e a redução de disparidades como questões centrais na governança de tecnologias em saúde. Dessa perspectiva, políticas de certificação não devem ser avaliadas somente pela quantidade de credenciais emitidas, mas pela capacidade de preservar e ampliar acesso a cuidados e informações de maneira segura.

A exigência irrestrita de certificação qualificada para pacientes também seria desproporcional em diversos fluxos e tenderia a excluir pessoas sem dispositivos, conectividade, documentos ou letramento digital suficientes. Por isso, a alternativa mais adequada é projetar níveis de garantia de identidade segundo o risco da operação, mantendo opções assistidas, acessibilidade e mecanismos seguros não dependentes de aquisição individual de certificados. A classificação jurídica da Lei nº 14.063/2020 oferece a base para essa abordagem escalonada.

5. PROPOSTA DE MATRIZ DE GOVERNANÇA DA CONFIANÇA DIGITAL

Com base na síntese anterior, propõe-se uma matriz analítico-operacional destinada a apoiar planos municipais, estaduais e federais de saúde digital. A matriz não constitui modelo empiricamente validado, nem norma mandatória: trata-se de contribuição propositiva que organiza requisitos de implantação e hipóteses para avaliação em ambientes reais. Sua unidade de análise é o fluxo de informação assistencial ou administrativo, e não apenas a quantidade de certificados digitais disponíveis.

A arquitetura conceitual compreende cinco camadas interdependentes: (i) identificação e prova de identidade; (ii) autenticação de sujeitos e sistemas, com assinatura conforme exigência aplicável; (iii) autorização por papéis, vínculos e finalidade; (iv) interoperabilidade sintática e semântica, incluindo padrões de registros; e (v) governança transversal de privacidade, auditoria, capacitação, continuidade de serviço e inclusão. Falhas em uma dessas camadas podem comprometer a confiabilidade do serviço mesmo quando a criptografia ou a assinatura funcionam adequadamente.

Quadro 2. Matriz proposta de confiança digital no SUS

Dimensão	**Requisito de governança**	**Instrumento de avaliação sugerido**
Identidade e credenciais	Verificação da identidade, escopo, validade e revogação.	Inventário de credenciais ativas e responsáveis; registros de rotação e revogação.

Assinaturas e atos	Nível de assinatura compatível com o documento e a norma.	Amostra de documentos com validação de autoria e integridade.
Autorização e privacidade	Privilégio mínimo, finalidade, base legal e trilhas auditáveis.	Revisões de perfis, logs de acesso e avaliações de conformidade.
Interoperabilidade	Integração homologada e dados semanticamente válidos.	Testes FHIR, taxas de rejeição e completude dos registros.
Equidade e capacidade	Canais assistidos, acessibilidade e suporte interfederativo.	Análise de barreiras, formação e continuidade de atendimento.
Governança e resultados	Monitoramento de incidentes, custos e resultados de cuidado.	Painel de indicadores e reavaliações periódicas.

Fonte: elaboração dos autores, com base nos documentos e estudos referenciados (2026).

5.1. Fases de Implementação e Responsabilidades

A implantação pode ser organizada em quatro fases incrementais. Na primeira, o ente público mapeia fluxos de dados, sistemas envolvidos, responsáveis, bases legais e categorias de documentos; realiza diagnóstico de infraestrutura, riscos e barreiras de acesso. Na segunda, define políticas de identidade, certificados, assinaturas, autorização, suporte e contratação, além de preparar os padrões clínicos e as interfaces exigidos pela RNDS. Na terceira, conduz projeto-piloto com homologação técnica e participação de trabalhadores da saúde, gestores e representantes de usuários. Na quarta, amplia de forma progressiva a integração e publica

indicadores agregados de desempenho, qualidade, segurança e acessibilidade.

A responsabilidade pela governança não deve ser delegada exclusivamente à equipe de tecnologia da informação. Gestores de saúde precisam definir finalidade, legitimidade e prioridade dos fluxos; profissionais assistenciais devem validar adequação clínica e usabilidade; equipes jurídicas e de proteção de dados devem examinar bases legais e contratos; profissionais de segurança devem estabelecer controles e contingências; e instâncias de participação social devem ser ouvidas quanto a acessibilidade, transparência e direitos dos cidadãos. A coordenação entre os níveis federativos é requisito de sustentabilidade, particularmente em municípios de pequeno e médio porte.

5.2. Indicadores para Avaliação de Resultados

A avaliação proposta deve estabelecer uma linha de base antes do piloto, preservar comparabilidade temporal e documentar custos, intervenções simultâneas e mudanças nos processos. Indicadores operacionais são necessários, mas não substituem desfechos assistenciais nem autorizam inferir causalidade. As metas numéricas devem ser pactuadas conforme capacidade e maturidade locais, não extraídas arbitrariamente de experiências incomparáveis.

Quadro 3. Indicadores sugeridos para acompanhamento

Indicador	**Definição operacional e periodicidade**	**Finalidade**
Credenciais regulares (%)	Credenciais válidas e vinculadas a titulares/entes autorizados ÷	Controle de identidade e ciclo de vida.

	total de credenciais em uso; mensal.	
Integrações homologadas (%)	Fluxos homologados com requisitos RNDS cumpridos ÷ fluxos previstos; trimestral.	Maturidade de interoperabilidade.
Rejeição técnica de registros (%)	Mensagens rejeitadas por erro de validação ÷ mensagens transmitidas; mensal.	Qualidade da integração e padrões.
Revisão de permissões (%)	Perfis de acesso revisados no prazo ÷ perfis sujeitos à revisão; trimestral.	Controle de autorização.
Incidentes por volume de operações	Incidentes confirmados por 100 mil operações, com tipificação; trimestral.	Monitoramento de segurança sem ocultar denominador.
Acesso assistido e inclusão	Percentual de usuários que necessitaram de suporte e taxa de conclusão dos serviços; semestral.	Detecção de barreiras digitais.
Continuidade do cuidado	Proporção de atendimentos com informações prévias acessíveis quando clinicamente necessárias; semestral.	Aferição de valor assistencial da integração.

Fonte: elaboração dos autores, com base nos documentos e estudos referenciados (2026).

6. DISCUSSÃO: CONTRIBUIÇÃO PARA A GESTÃO PÚBLICA E A SAÚDE DIGITAL

A principal inferência desta pesquisa é que a confiança digital em saúde possui natureza sociotécnica e institucional. A perspectiva crítica de Massonetto, Bachur e Carvalho (2020) contribui para problematizar modelos de cidade inteligente nos quais a eficiência

instrumental se sobrepõe à autonomia dos sujeitos. Em política sanitária, o critério de sucesso não pode restringir-se à redução de atritos administrativos: deve incluir garantias de direitos, participação e acesso efetivo. Moldero et al. (2026), ao discutirem o cuidado oportuno em contextos de escassez, mostram a pertinência de vincular governança, critérios verificáveis de regulação e efeitos territoriais sobre os pacientes. Ela depende simultaneamente de provas de identidade, controles de acesso, regras de uso legítimo da informação, legibilidade semântica dos registros e capacidade de prestação de contas. Uma política restrita à compra e distribuição de certificados pode aumentar o número de credenciais sem alterar os problemas essenciais de fragmentação de dados ou de continuidade assistencial. Por outro lado, integrar a certificação a políticas de governança pode favorecer a segurança de interações e a verificabilidade de atos em fluxos que efetivamente demandam tal nível de garantia.

Essa interpretação fortalece a convergência entre a literatura jurídica, as diretrizes de informática em saúde e as pesquisas em gestão pública. No plano local, Silva (2023) e Silva, Trindade e Barbosa (2023) ressaltam que o valor dos dados do SUS se manifesta quando sua qualidade e sua utilização apoiam planejamento, distribuição de recursos e decisões territorializadas. No plano nacional, Haddad e Lima (2024) e os documentos ministeriais articulam a saúde digital à reorganização do SUS. No plano técnico, o DATASUS distingue credenciamento de aplicações e troca de informações conforme os serviços e padrões disponibilizados. A matriz proposta integra essas contribuições sem reduzir governança à solução criptográfica.

Também se evidencia uma ligação com o uso crescente de inteligência artificial em sistemas públicos de saúde. Silva, Trindade e Barbosa (2026) discutem aplicações e limitações da IA na gestão. Sistemas analíticos e algoritmos não se tornam confiáveis pelo simples fato de consumirem dados provenientes de canais autenticados. A procedência técnica deve ser acompanhada de qualidade do registro, legitimidade do tratamento, avaliação de vieses e supervisão humana. A certificação pode sustentar uma dimensão da proveniência, mas não fornece, isoladamente, validação clínica, consistência estatística ou justiça distributiva.

No plano regulatório, a escolha de mecanismos deve respeitar proporcionalidade. A lei brasileira admite diferentes níveis de assinatura eletrônica e prevê tratamento diferenciado conforme os atos envolvidos; a LGPD exige justificativa, limitação de finalidade e salvaguardas. A adoção de certificados deve, portanto, decorrer de uma decisão baseada em risco, natureza documental, obrigações concretas e condições de acesso. Esse enfoque evita impor custos a pacientes sem necessidade jurídica e reduz o perigo de transformar a tecnologia em requisito impeditivo de atendimento.

A experiência de Recife e Ebserh relatada por Pinto et al. (2025) reforça a relevância de modelos de federação de dados que respondam à fragmentação informacional. Sua transferibilidade, contudo, requer análise de contexto. Municípios podem diferir significativamente quanto a arquitetura legada, quadro de pessoal, contratos, infraestrutura e escala assistencial. O Decreto nº 12.560/2025 e a estratégia de municipalização da RNDS criam um ambiente institucional favorável à coordenação; a realização de seus objetivos deve ser verificada por indicadores e estudos de implementação, e não presumida a partir da existência da norma.

Por fim, é necessário distinguir uma hipótese plausível de um efeito demonstrado. O manuscrito anterior atribuía reduções percentuais de irregularidades à adoção de certificados e apresentava um índice de conectividade sem correspondência verificável nas referências utilizadas. A presente versão elimina essas estatísticas, preservando apenas resultados associados a fontes identificáveis. Esta decisão não enfraquece a tese central; delimita seu alcance e indica qual evidência adicional seria necessária para demonstrar impacto sobre segurança, custos, confiança cidadã e qualidade do cuidado.

7. LIMITAÇÕES E AGENDA DE PESQUISA

A principal limitação é a natureza narrativa e documental do estudo. A seleção intencional de fontes, embora rastreável, não substitui buscas sistemáticas com registro integral de estratégias, triagem por revisores independentes e avaliação formal de risco de viés. Ademais, guias e normas informam requisitos pretendidos, não a efetividade de seu cumprimento em todos os estabelecimentos. Os estudos empíricos utilizados tratam de informatização e interoperabilidade mais amplas, e não de experimentos que isolem a certificação digital como intervenção independente.

Propõe-se que pesquisas futuras empreguem desenhos de implementação em redes municipais e regionais, com comparação pré e pós-implantação, grupo de comparação quando viável, séries temporais interrompidas ou métodos mistos. As variáveis de interesse podem abranger incidentes de autenticação, validade de assinaturas, erros de integração, tempo de obtenção de informações clínicas, custo total de propriedade, satisfação de trabalhadores e usuários e desigualdades de acesso. A coleta deverá atender às

bases legais, aos critérios éticos e aos protocolos de proteção de dados aplicáveis.

Outra linha de pesquisa consiste em examinar a relação entre custódia de certificados, terceirização de sistemas, governança do acesso e resposta a incidentes em organizações com diferentes níveis de maturidade. Também é pertinente analisar os impactos distributivos da digitalização sobre pessoas idosas, pessoas com deficiência e populações territorialmente vulneráveis, distinguindo disponibilidade do serviço, capacidade efetiva de utilização e resultados de cuidado.

8. CONSIDERAÇÕES FINAIS

O artigo examinou a certificação digital como componente de uma infraestrutura de confiança necessária à transformação digital do SUS, sem atribuir à tecnologia capacidades que dependem de outros mecanismos. A análise do marco regulatório e da documentação técnica confirma a relevância da ICP-Brasil para autenticação institucional e assinaturas qualificadas em contextos previstos, inclusive na conexão de estabelecimentos com a RNDS. Ao mesmo tempo, a proteção de dados, a autorização de acessos e a interoperabilidade clínica exigem controles, padrões e responsabilidades adicionais.

As evidências científicas verificadas demonstram evolução dos prontuários eletrônicos e experiências reais de integração no sistema público, mas não sustentam generalizações causais sobre redução de fraudes, economia de recursos ou melhoria assistencial decorrentes exclusivamente da certificação. O principal resultado propositivo é uma matriz de governança que combina identidade,

assinaturas, autorização, interoperabilidade, privacidade, capacidades administrativas, equidade e mensuração de resultados.

Recomenda-se que o planejamento interfederativo da saúde digital priorize fluxos assistenciais de maior valor público, adote autenticação e assinaturas proporcionais aos riscos, proteja a autonomia informacional dos cidadãos e mantenha alternativas inclusivas de acesso. A modernização do SUS será mais consistente quando confiança digital deixar de significar apenas validade criptográfica e passar a representar um atributo demonstrável de sistemas, instituições e relações de cuidado. Essa é a condição para converter tecnologia em capacidade pública, e capacidade pública em benefício social.

REFERÊNCIAS BIBLIOGRÁFICAS

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo: tratamento de dados pessoais pelo Poder Público. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 6 nov. 2026.

BRASIL. Decreto nº 12.560, de 23 de julho de 2025. Dispõe sobre a Rede Nacional de Dados em Saúde e sobre as Plataformas SUS Digital. Brasília, DF, 2025. Disponível em: https://legislacao.presidencia.gov.br/atos/?ano=2025&ato=6a3QTSq5UNZpWTb27&numero=12560&tipo=DEC. Acesso em: 6 nov. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em:

https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.html. Acesso em: 6 nov. 2026.

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde. Brasília, DF, 2020b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm. Acesso em: 6 nov. 2026.

BRASIL. Lei nº 8.080, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde [...]. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 6 nov. 2026.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Brasília, DF, 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 6 nov. 2026.

BRASIL. Ministério da Saúde. Estratégia de Saúde Digital para o Brasil 2020–2028. Brasília, DF: Ministério da Saúde, 2020a. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 6 nov. 2026.

BRASIL. Ministério da Saúde. Portaria GM/MS nº 3.232, de 1º de março de 2024. Institui o Programa SUS Digital. Brasília, DF, 2024. Disponível em: https://bvs.saude.gov.br/bvs/saudelegis/gm/2024/prt3232_04_03_2024.html. Acesso em: 6 nov. 2026.

CELUPPI, Ianka Cristina et al. Dez anos do Prontuário Eletrônico do Cidadão e-SUS APS: em busca de um Sistema Único de Saúde eletrônico. Revista de Saúde Pública, São Paulo, v. 58, 2024. DOI: https://doi.org/10.11606/s1518-8787.2024058005770.

DATASUS. WEB Atendimento SUS: perguntas frequentes sobre a Rede Nacional de Dados em Saúde. Brasília, DF: Ministério da Saúde, [s.d.]. Disponível em: https://webatendimento.saude.gov.br/faq/rnds. Acesso em: 6 nov. 2026.

GONÇALO, Wemerson; SOUZA, Maria Clara de; SANTOS, Wellington Pinheiro dos; OLIVEIRA, Fábio Henrique Cavalcanti de. Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023. Physis: Revista de Saúde Coletiva, v. 35, n. 1, e350113, 2025. DOI: https://doi.org/10.1590/S0103-73312025350113pt.

HADDAD, Ana Estela; LIMA, Nísia Trindade. Saúde Digital no Sistema Único de Saúde (SUS). Interface – Comunicação, Saúde, Educação, Botucatu, v. 28, e230597, 2024. DOI: https://doi.org/10.1590/interface.230597.

HL7 INTERNATIONAL. HL7 FHIR Release 4: Fast Healthcare Interoperability Resources. Ann Arbor, 2019. Disponível em: https://hl7.org/fhir/R4/. Acesso em: 6 nov. 2026.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Assinatura eletrônica avançada. Brasília, DF: ITI, 2024. Disponível em: https://www.gov.br/iti/pt-br/assuntos/assinatura-eletronica-avancada/assinatura-eletronica-avancada. Acesso em: 6 nov. 2026.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Certificado digital. Brasília, DF: ITI, 2026. Disponível em:

https://www.gov.br/iti/pt-br/assuntos/icp-brasil/certificado-digital. Acesso em: 6 nov. 2026.

LUCENA, Fábio Nogueira de et al. Certificado digital. 2. ed. Goiânia: Cegraf UFG, 2023. DOI: https://doi.org/10.5216/CER.ebook.978-85-495-0693-1/2023.

MASSONETTO, Luís Fernando; BACHUR, João Paulo; CARVALHO, Eduardo de Moraes. Reificação da experiência na cidade inteligente: notas para uma crítica da economia política do espaço urbano. Revista Direito e Práxis, v. 11, n. 1, p. 591–611, 2020. DOI: https://doi.org/10.1590/2179-8966/2020/48205.

MINISTÉRIO DA SAÚDE. Certificado digital: Guia da RNDS para o gestor. Brasília, DF: Ministério da Saúde, [s.d.]-a. Disponível em: https://rnds-guia.saude.gov.br/docs/publico-alvo/gestor/certificado/. Acesso em: 6 nov. 2026.

MINISTÉRIO DA SAÚDE. Guia de Implementação da Rede Nacional de Dados em Saúde (RNDS): padrão HL7 FHIR R4. Brasília, DF: Ministério da Saúde, [s.d.]-b. Disponível em: https://fhir.saude.gov.br/. Acesso em: 6 nov. 2026.

MINISTÉRIO DA SAÚDE. Mais de 87% das Unidades Básicas de Saúde utilizam prontuário eletrônico e quase a totalidade tem acesso à internet. Brasília, DF, 18 jun. 2025. Disponível em: https://www.gov.br/saude/pt-br/assuntos/noticias/2025/junho/mais-de-87-das-unidades-basicas-de-saude-utilizam-prontuario-eletronico-e-quase-a-totalidade-tem-acesso-a-internet. Acesso em: 6 nov. 2026.

MINISTÉRIO DA SAÚDE. Ministério da Saúde apresenta estratégia sobre Rede Nacional de Dados em Saúde. Brasília, DF, 14 jul. 2026. Disponível em: https://www.gov.br/saude/pt-br/assuntos/noticias/2026/julho/ministerio-da-saude-apresenta-estrategia-sobre-rede-nacional-de-dados-em-saude. Acesso em: 6 nov. 2026.

MOLDERO, Leonardo de Souza; SILVA, Moisés Figueiredo da; LEITE, Tiago Simões; TRINDADE, Luciano Henrique; BARBOSA, Antônio Pires. Cuidado oportuno, escassez regulada e direitos dos pacientes nas cidades resilientes. Revista Tópicos, v. 4, n. 38, p. 1–93, 2026. DOI: https://doi.org/10.70773/revistatopicos/793076602.

NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Digital Identity Guidelines: NIST Special Publication 800-63-4. Gaithersburg: NIST, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-63-4.

OMS – ORGANIZAÇÃO MUNDIAL DA SAÚDE. Global strategy on digital health 2020–2027. Geneva: WHO, 2025. ISBN 978-92-4-011687-0. Disponível em: https://www.who.int/publications/i/item/9789240116870. Acesso em: 6 nov. 2026.

ORRILLO, Yansy Aurora Delgado; SANTOS, Romário Correia dos; DANTAS, Erica Simone Barbosa; CACERES, Felix Hector Rigoli. Percepção de gestores públicos de saúde sobre a transformação digital do SUS: estudo de caso. Saúde em Debate, v. 49, n. esp. 1, 2025. DOI: https://doi.org/10.1590/2358-28982025E19928P.

PINTO, Hêider Aurélio et al. Superando a histórica fragmentação de dados no SUS: interoperabilidade em Recife e na Ebserh. Saúde em

Debate, Rio de Janeiro, v. 49, n. esp. 1, 2025. DOI: https://doi.org/10.1590/2358-28982025E110011P.

SILVA, Moisés Figueiredo da; MOLDERO, Leonardo de Souza; TRINDADE, Luciano Henrique; BARBOSA, Antônio Pires. Percurso metodológico para revisões sistemáticas em ciências sociais aplicadas: desafios, estratégias e impactos. ARACÊ, v. 6, n. 4, p. 18600–18617, 2024. DOI: https://doi.org/10.56238/arev6n4-443.

SILVA, Moisés Figueiredo da; TRINDADE, Luciano Henrique; BARBOSA, Antônio Pires. A importância do uso de indicadores do SUS para o planejamento de serviços de saúde no município de Ilhabela/SP. Revista de Direito da Administração Pública, v. 1, n. 2, 2023. Disponível em: https://centrodeestudosdedireito.com.br/revistas/index.php/redap/article/view/23. Acesso em: 6 nov. 2026.

SILVA, Moisés Figueiredo da; TRINDADE, Luciano Henrique; BARBOSA, Antônio Pires. Inteligência artificial na saúde pública: inovações, desafios e aplicações para melhoria da gestão. Revista Tópicos, Rio de Janeiro, v. 4, n. 37, p. 1–31, 2026. DOI: https://doi.org/10.70773/revistatopicos/790563601.

SILVA, Moisés Figueiredo da. O uso de indicadores do Sistema Único de Saúde para o planejamento de serviços públicos de saúde no município de Ilhabela/SP. 2023. 65 f. Dissertação (Mestrado em Cidades Inteligentes e Sustentáveis) – Universidade Nove de Julho, São Paulo, 2023. Disponível em: https://bibliotecatede.uninove.br/handle/tede/3163. Acesso em: 6 nov. 2026.

[1] Advogado. Mestrando no programa de pós-graduação stricto sensu em Cidades Inteligentes e Sustentáveis da Universidade Nove de Julho. Especialista em Gestão Pública pelo Instituto Federal do Espírito Santo – IFES. Graduado em Direito pela Universidade Federal do Espírito Santo – UFES. ORCID: https://orcid.org/0009-0000-4476-2291. E-mail: acesse o artigo original para visualizar o e-mail

[2] Advogado. Mestrando no programa de pós-graduação stricto sensu em Cidades Inteligentes e Sustentáveis da Universidade Nove de Julho. Aluno do programa de pós-graduação lato sensu em Direito Médico e Biomédico da Escola Brasileira de Direito. Especialista em compliance, auditoria interna e ESG. Graduado em Direito pela Universidade São Judas Tadeu. ORCID: https://orcid.org/0009-0004-8815-7682. E-mail: acesse o artigo original para visualizar o e-mail.

[3] Doutorando e Mestre em Cidades Inteligentes e Sustentáveis pela Universidade Nove de Julho – UNINOVE, Especialista em Administração Pública e Gerência de Cidades, Graduado em Gestão Pública. ORCID: https://orcid.org/0000-0002-3012-3402. E-mail: acesse o artigo original para visualizar o e-mail.

[4] Doutor em Direito, Instituição: Universidade Nove de Julho (Uninove), Universidade de São Paulo (USP). ORCID: https://orcid.org/0000-0002-0250-5614. E-mail: acesse o artigo original para visualizar o e-mail.

[5] Doutor e Mestre em Administração de Empresas pela Fundação Getúlio Vargas – FGV, graduado em Medicina, professor titular do Programa de Mestrado Profissional em Gestão de Sistemas de

Saúde e do Programa de Mestrado Acadêmico em Gestão de Cidades Inteligentes e Sustentáveis da Universidade Nove de Julho, além de docente do Programa de Graduação em Medicina na área de Saúde Coletiva e Atenção Primária em Saúde. ORCID: https://orcid.org/0000-0001-6478-6522. E-mail: acesse o artigo original para visualizar o e-mail.