

**Sociedade Brasileira de Informática em Saúde - SBIS**  
**Nota Técnica - Infraestrutura Pública Digital Setorial em Saúde**  
**PRL-8 PL nº 5.875/2013**

**Contribuições Técnicas da SBIS ao PRL-8 do PL nº 5.875/2013: síntese objetiva e fundamentação detalhada**

Este documento reúne as contribuições técnicas da Sociedade Brasileira de Informática em Saúde (SBIS) ao debate sobre o PRL-8 do PL nº 5.875/2013, relativo à infraestrutura pública digital setorial em saúde.

A primeira parte apresenta uma síntese objetiva dos principais pontos recomendados, com a finalidade de facilitar a leitura, a deliberação institucional e a identificação rápida dos temas prioritários. A segunda parte apresenta a Nota Técnica detalhada, com a fundamentação técnica, jurídica, arquitetural e institucional das contribuições.

**1. Síntese objetiva das contribuições técnicas da SBIS: principais pontos para consideração no aprimoramento do PRL-8.**

- Explicitar que a RNDS deve atuar como plataforma nacional de interoperabilidade, coordenação, governança e troca segura de informações em saúde, e não como repositório centralizador integral de dados clínicos identificados.
- Reforçar a governança da infraestrutura pública digital em saúde, com definição clara de responsabilidades entre União, estados, municípios, prestadores públicos e privados, fornecedores tecnológicos, controladores, operadores e instâncias de auditoria.
- Preservar prioritariamente os dados clínicos identificados nos sistemas de origem, garantindo integridade, disponibilidade, rastreabilidade, segurança, portabilidade, versionamento e auditabilidade.
- Detalhar, em regulamentação específica, quais conjuntos mínimos de dados devem ser obrigatoriamente compartilhados com a RNDS para garantir a continuidade do cuidado.
- Adotar padrões nacionais e internacionais amplamente reconhecidos, preferencialmente abertos, interoperáveis, sustentáveis e desenvolvidos por processos técnicos baseados em consenso.
- Fortalecer mecanismos de transparência, incluindo registros de acesso auditáveis, identificação de quem acessou os dados, instituição vinculada, perfil de acesso, data, hora, finalidade, base legal e eventual compartilhamento subsequente.
- Prever requisitos mínimos de continuidade operacional, incluindo backup, recuperação de desastres, planos de contingência, redundância, migração segura, exportação em padrões interoperáveis e preservação de dados em eventos críticos.
- Evitar apagamento, substituição ou sobrescrita silenciosa de registros clínicos, assegurando versionamento, justificativa técnica, rastreabilidade e preservação do histórico quando necessário.
- Criar salvaguardas para uso secundário de dados em pesquisa, inovação, avaliação de políticas públicas e desenvolvimento tecnológico, com base legal adequada, minimização, anonimização ou pseudonimização quando aplicável, avaliação de impacto e auditoria.

- Prever governança específica para aplicações de inteligência artificial baseadas em dados da RNDS ou de sistemas conectados, incluindo avaliação de risco, validação, explicabilidade proporcional ao risco, monitoramento pós-implantação, mitigação de vieses e responsabilização institucional.
- Estabelecer regras para modelos de negócio baseados em dados de saúde, vedando usos incompatíveis com finalidades assistenciais, sanitárias ou públicas e exigindo transparência, responsabilização e gestão de conflitos de interesse.
- Fortalecer instâncias colegiadas multissetoriais permanentes, com participação de entes federativos, comunidade científica, profissionais de saúde, setor produtivo, sociedade civil, órgãos reguladores e especialistas em saúde digital.
- Prever financiamento, sustentabilidade econômica, capacidade institucional e formação continuada de profissionais e gestores como condições para implementação efetiva da infraestrutura pública digital em saúde.
- Instituir ou fortalecer serviço nacional de terminologias em saúde, apoiando interoperabilidade semântica, qualidade dos dados, recuperação da informação, gestão, assistência, pesquisa e inovação.

## **2. Nota Técnica detalhada**

### **2.1. Introdução e Contexto Estratégico**

A construção de uma infraestrutura nacional de dados em saúde representa uma decisão estratégica de longo prazo, com impactos relevantes sobre a sustentabilidade do sistema, a proteção de dados pessoais, a coordenação interfederativa e a capacidade de inovação do ecossistema digital em saúde.

Nesse contexto, a Sociedade Brasileira de Informática em Saúde (SBIS) apresenta, em espírito colaborativo e técnico, contribuições ao debate sobre o Substitutivo ao PL nº 5.875/2013 (PRL-8), atualmente em apreciação na Comissão de Saúde da Câmara dos Deputados. A transformação digital da saúde exige modelos institucionais capazes de equilibrar interoperabilidade, segurança, escalabilidade, governança compartilhada e proteção dos direitos do cidadão.

A infraestrutura pública digital em saúde deve assegurar não apenas o compartilhamento seguro de informações, mas também a preservação longitudinal, íntegra, disponível e auditável dos dados clínicos ao longo do tempo. Essa infraestrutura deve ser sustentada por uma governança clara, transparente, multissetorial e contínua, capaz de definir as responsabilidades, os papéis institucionais, os critérios de acesso, os mecanismos de supervisão, a auditoria independente e a prestação de contas.

Do ponto de vista técnico, essa governança deve estar apoiada em uma infraestrutura orientada à saúde, composta por arquitetura, comunicação, terminologias, segurança da informação e padrões nacionais e internacionais que garantam interoperabilidade sintática, semântica e

operacional. Em saúde, a perda, a sobrescrita indevida, a inacessibilidade ou o desaparecimento silencioso de dados pode comprometer a continuidade do cuidado, a segurança do paciente, a responsabilidade profissional, a vigilância em saúde, a pesquisa, a gestão pública e os direitos do titular dos dados.

## **2.2 Contexto Arquitetural**

A definição da arquitetura, de seus componentes, fluxos, responsabilidades e mecanismos de governança da RNDS é central para a consolidação de um ecossistema digital interoperável, seguro, auditável e sustentável no SUS. Experiências internacionais demonstram que arquiteturas federadas, nas quais os dados permanecem sob custódia dos sistemas de origem e são compartilhados mediante camadas interoperáveis, podem favorecer auditabilidade, distribuição de responsabilidades, resiliência operacional, continuidade do cuidado e fortalecimento do federalismo cooperativo, desde que acompanhadas de governança transparente, multissetorial e com clara definição de papéis institucionais.

Nesse modelo, a RNDS deve atuar como plataforma nacional de interoperabilidade, coordenação e troca segura de informações em saúde, provendo padrões abertos, autenticação, autorização, rastreabilidade, registro de acessos, serviços terminológicos e mecanismos de governança para uma rede distribuída de dados, sem necessidade de centralização integral dos registros clínicos identificados.

A opção por uma arquitetura federada exige, contudo, salvaguardas técnicas, jurídicas e institucionais explícitas, de modo que a permanência dos dados nos sistemas de origem não resulte em fragmentação, perda de disponibilidade, inconsistência, inacessibilidade ou descontinuidade do histórico clínico. Para isso, os sistemas de origem devem assegurar autenticidade, integridade, disponibilidade, confidencialidade, versionamento, backup, recuperação de desastres, portabilidade, exportação em padrões abertos e trilhas de auditoria.

Essas obrigações devem estar vinculadas a uma governança clara, com definição de responsabilidades entre controladores, operadores, entes federativos, prestadores públicos e privados e fornecedores tecnológicos, inclusive em situações de migração tecnológica, troca de fornecedor, encerramento de atividades, fusão de cadastros, substituição de sistemas ou descontinuidade contratual.

## **2.3. Referências Internacionais**

O Brasil participou ativamente da formulação de princípios internacionais relacionados à Infraestrutura Pública Digital durante a presidência do G20 em 2024. Esse debate reforça a necessidade de que infraestruturas públicas digitais setoriais, como a de saúde, sejam desenhadas

com governança multissetorial, transparente, participativa e sustentável, assegurando interoperabilidade, segurança, inclusão, equidade, rastreabilidade, proteção de direitos e continuidade institucional.

Diversas jurisdições têm demonstrado a viabilidade operacional de modelos de infraestrutura digital baseados em coordenação institucional, padrões interoperáveis e governança federada. A Estônia opera, desde 2001, o X-Road; a Suécia organiza sua saúde digital em modelo regional coordenado pela Inera; Canadá, Austrália e Dinamarca adotam estruturas colegiadas de governança interfederativa; e a Índia consolidou modelo de interoperabilidade em larga escala baseado em APIs. Essas experiências demonstram que modelos descentralizados, interoperáveis e orientados por padrões obtidos por consenso, preferencialmente abertos e sustentáveis, podem coexistir com elevada eficiência operacional, segurança, auditabilidade e capacidade de inovação.

Embora esses modelos não sejam diretamente transponíveis ao contexto brasileiro, oferecem referências úteis sobre governança federada, coordenação multissetorial, definição de responsabilidades, autenticação, autorização, rastreabilidade, interoperabilidade e sustentabilidade institucional. Para o SUS, essas referências reforçam a importância de uma governança capaz de equilibrar coordenação nacional, autonomia federativa, participação social, segurança jurídica, inovação tecnológica e proteção dos direitos dos titulares de dados.

A transparência deve ser operacionalizada por meio de registros de acesso rastreáveis, auditáveis e protegidos contra alteração indevida, permitindo ao titular dos dados identificar quem acessou suas informações, a instituição vinculada, o perfil de acesso, a data e hora, a finalidade declarada, a base legal aplicável, o conjunto de dados consultado e eventual compartilhamento subsequente. Esses registros devem ser preservados por prazo adequado, disponibilizados ao titular em linguagem acessível e submetidos a mecanismos de auditoria por autoridades competentes e instâncias independentes, quando aplicável.

#### **2.4. Aspectos Técnicos Relevantes**

À luz das melhores práticas internacionais e da realidade federativa brasileira, alguns aspectos do PRL-8 podem ser aprimorados para fortalecer sua aderência aos princípios de governança digital sustentável.

A institucionalização de instâncias colegiadas permanentes envolvendo União, estados, municípios, comunidade científica, setor produtivo, terceiro setor, sociedade civil e órgãos reguladores pode contribuir para maior legitimidade, continuidade e efetividade da política nacional de saúde digital.

A adoção explícita de padrões nacionais e internacionais amplamente reconhecidos, desenvolvidos por processos técnicos, transparentes e baseados em consenso, favorece a integração

entre sistemas heterogêneos, reduz dependências tecnológicas, amplia a competição, estimula a inovação e fortalece a sustentabilidade do ecossistema digital em saúde. Nesse sentido, recomenda-se também ampliar a participação sistemática de especialistas brasileiros em organismos nacionais e internacionais de normalização, de modo a contribuir para a construção, adaptação e atualização de normas aplicáveis à saúde digital.

A preservação prioritária dos dados clínicos identificados nos sistemas de origem pode fortalecer a auditabilidade, a rastreabilidade, a qualidade dos dados e a distribuição de responsabilidades no ecossistema digital do SUS. Esse modelo contribui para que o dado seja qualificado no ponto em que é produzido, reduzindo riscos de perda de contexto clínico, inconsistência, duplicidade ou dependência excessiva de repositórios centralizados.

A separação entre funções operacionais, normativas, fiscalizatórias e de auditoria independente constitui boa prática de governança institucional, pois reduz conflitos de interesse, amplia a transparência decisória e fortalece a responsabilização dos atores públicos e privados envolvidos na infraestrutura digital em saúde.

Os fluxos de tratamento de dados pessoais sensíveis em saúde devem observar a LGPD, incluindo os princípios de finalidade, adequação, necessidade, segurança, prevenção, responsabilização e prestação de contas. Para isso, é indispensável definir de forma clara os papéis de controladores, operadores e, quando aplicável, situações de controladoria conjunta, especialmente nos processos de compartilhamento, uso secundário, interoperabilidade, auditoria, pesquisa, inovação e gestão pública.

Para isso, é indispensável definir de forma clara os papéis de controladores, operadores e, quando aplicável, situações de controle conjunto, especialmente nos processos de compartilhamento, uso secundário, interoperabilidade, auditoria, pesquisa, inovação e gestão pública.

## **2.5. Pontos de Atenção Relacionados à Arquitetura e Governança de Dados**

Considerando a relevância estratégica da RNDS para a continuidade do cuidado, a sustentabilidade do SUS e a proteção dos direitos dos titulares de dados, alguns pontos merecem aprofundamento técnico e regulatório adicional no âmbito do Art.4º e do Art.8º do PRL-8.

O Art. 4º prevê a utilização de modelos publicados pelo Ministério da Saúde para a interoperabilidade da RNDS. Recomenda-se, contudo, explicitar de forma mais objetiva que tais modelos devem observar padrões nacionais e internacionais amplamente reconhecidos, preferencialmente abertos, interoperáveis, sustentáveis e desenvolvidos por processos técnicos baseados em consenso, em articulação com organismos de normalização competentes, incluindo,

quando aplicável, o Sistema Nacional de Metrologia, Normalização e Qualidade Industrial - Sinmetro.

A adoção explícita de padrões de interoperabilidade nacionais e internacionais, amplamente reconhecidos e preferencialmente abertos, pode contribuir para neutralidade tecnológica, a redução de dependência de fornecedores específicos, a sustentabilidade de longo prazo, a ampliação da competição, a inovação responsável e a integração entre ecossistemas públicos e privados de saúde. A governança técnica baseada em padrões desenvolvidos por processos transparentes, técnicos e consensuais favorece escalabilidade, interoperabilidade, segurança institucional, previsibilidade regulatória e confiança no ecossistema digital em saúde.

O Art. 8º reconhece a custódia primária dos dados nos sistemas de origem, ao mesmo tempo em que prevê o envio de informações à RNDS. Nesse contexto, recomenda-se explicitar de forma mais objetiva o papel da RNDS como plataforma nacional de interoperabilidade, coordenação, governança e troca segura de informações em saúde evitando interpretações que possam caracterizá-la como repositório centralizador integral de dados clínicos identificados.

Dados clínicos pessoais, especialmente aqueles identificados ou identificáveis, devem ser preservados prioritariamente nos sistemas de origem, observadas as hipóteses legais de compartilhamento, interoperabilidade e tratamento secundário previstas na legislação aplicável. Essa preservação deve estar associada a requisitos mínimos de integridade, disponibilidade, rastreabilidade, segurança, portabilidade, versionamento e auditoria.

As experiências internacionais analisadas sugerem que arquiteturas federadas e interoperáveis, quando acompanhadas de governança clara e mecanismos robustos de responsabilização, tendem a favorecer maior resiliência operacional, distribuição de responsabilidades, escalabilidade, segurança jurídica e continuidade do cuidado.

Ainda sobre o Art. 8º, há menção ao envio obrigatório à RNDS das informações necessárias à continuidade do cuidado. Considerando a relevância jurídica, assistencial e operacional dessa definição, recomenda-se maior detalhamento técnico e normativo sobre quais conjuntos mínimos de dados deverão compor essa obrigatoriedade, preferencialmente por meio de regulamentação específica, com participação de instâncias técnicas, científicas, federativas e sociais.

A definição explícita de critérios técnicos, clínicos, operacionais, jurídicos e regulatórios pode contribuir para maior segurança jurídica aos entes participantes, redução de ambiguidades interpretativas, prevenção de assimetrias operacionais e mitigação de potenciais judicializações relacionadas à extensão do compartilhamento obrigatório de dados.

A manutenção dos dados nos sistemas onde foram originalmente gerados fortalece um modelo de saúde digital mais integrado, distribuído, seguro e aderente à lógica federativa do SUS.

No entanto, esse modelo exige mecanismos robustos de governança, continuidade operacional, segurança da informação e preservação longitudinal dos registros clínicos.

Recomenda-se, portanto, que os sistemas de origem assegurem requisitos mínimos de continuidade operacional, segurança da informação e preservação longitudinal dos registros clínicos, incluindo políticas de backup e recuperação de desastres, planos de contingência, redundância, versionamento, portabilidade, exportação em padrões interoperáveis, preferencialmente abertos, mecanismos de migração segura entre plataformas e trilhas de auditoria.

Esses requisitos devem contemplar situações ordinárias e excepcionais, como migração tecnológica, substituição de sistemas, troca ou encerramento de contratos, falência ou descontinuidade de fornecedores privados, fusão de cadastros e eventos climáticos extremos. O versionamento deve preservar alterações sucessivas do registro clínico, evitando apagamento, substituição ou sobrescrita silenciosa. As trilhas de auditoria devem documentar quem acessou, alterou, compartilhou ou excluiu informações, em que momento, por qual finalidade, com qual base legal e sob qual perfil de autorização.

Tais salvaguardas devem ser tratadas como componentes estruturantes da governança da infraestrutura pública digital em saúde, contribuindo para garantir disponibilidade contínua, integridade histórica, auditabilidade, segurança jurídica e proteção do patrimônio informacional em saúde.

## **2.6. Recomendações Técnicas**

Considerando as referências internacionais e os princípios já consolidados na governança digital contemporânea, recomenda-se avaliar:

- fortalecimento de instâncias colegiadas multissetoriais permanentes;
- ampliação de mecanismos de participação técnica e social;
- adoção e desenvolvimentos de padrões seguindo os princípios internacionais de desenvolvimento de normas por consenso para a interoperabilidade;
- preservação prioritária dos dados clínicos identificados nos sistemas de origem;
- mecanismos robustos de auditabilidade e rastreabilidade;
- ampliação de instrumentos digitais de transparência, gestão de preferências, portabilidade, registro de acessos e, quando juridicamente aplicável, consentimento;
- fortalecimento da atuação coordenada entre Ministério da Saúde, ANPD e entes federativos;
- definição de requisitos mínimos para logs transacionais, incluindo imutabilidade, carimbo temporal, identificação de acessos, finalidade, base legal e consulta pelo titular;

- garantia de preservação, integridade, disponibilidade, backup, versionamento e portabilidade dos dados clínicos nos sistemas de origem;
- previsão de mecanismos de correção de dados com versionamento, sem apagamento silencioso do histórico clínico;
- estabelecimento de regras para migração, substituição de sistemas, encerramento de contratos e troca de fornecedores, assegurando exportação em padrões abertos e continuidade do acesso aos dados;
- criação de salvaguardas específicas para uso secundário de dados em pesquisa, inovação, avaliação de políticas públicas e desenvolvimento tecnológico, incluindo base legal adequada, minimização de dados, governança ética, anonimização ou pseudonimização quando aplicável, avaliação de impacto e mecanismos de auditoria;
- previsão de governança específica para aplicações de inteligência artificial baseadas em dados da RNDS ou de sistemas conectados, incluindo avaliação de risco, validação, explicabilidade proporcional ao risco, monitoramento pós-implantação, mitigação de vieses, documentação técnica e responsabilização institucional.
- previsão de regras para modelos de negócio baseados em dados de saúde, vedando usos incompatíveis com a finalidade assistencial, sanitária ou pública, e exigindo transparência, responsabilização dos agentes envolvidos, gestão de conflitos de interesse e proteção dos direitos dos titulares;
- fortalecimento de mecanismos de auditoria independente, gestão de conflitos de interesse e responsabilização dos controladores públicos e privados;
- vedação ao apagamento, sobrescrita ou substituição de registros clínicos sem mecanismo de versionamento, justificativa técnica, rastreabilidade, trilha de auditoria e preservação do histórico quando clinicamente ou juridicamente necessário;
- adoção de um serviço de terminologia nacional que permita uma qualidade e completude na recuperação de dados para a gestão e pesquisa em saúde.

## **2.7. Considerações Finais**

O momento atual representa oportunidade estratégica para consolidação de um modelo brasileiro de saúde digital baseado em cooperação federativa, interoperabilidade, sustentabilidade institucional e confiança social.

Nesse contexto, o aprimoramento contínuo do PRL-8 pode contribuir para consolidar uma política nacional de saúde digital alinhada às melhores práticas globais, à legislação brasileira e aos compromissos multilaterais assumidos pelo país.

O avanço da RNDS deve preservar o equilíbrio entre coordenação nacional, autonomia federativa, segurança jurídica, proteção dos titulares, continuidade do cuidado, governança técnica transparente e sustentabilidade institucional. A definição legal da infraestrutura não deve cristalizar uma arquitetura excessivamente centralizadora nem deixar lacunas capazes de comprometer a integridade, a disponibilidade e a rastreabilidade longitudinal dos dados em saúde.

Além disso, a implementação da infraestrutura pública digital em saúde deve ser acompanhada de previsão clara de fontes de financiamento, mecanismos de sustentabilidade econômica, fortalecimento da capacidade institucional dos entes federativos e investimento continuado em capital humano. Isso inclui ambientes técnicos adequados, equipes qualificadas, formação permanente de profissionais e gestores, desenvolvimento de competências em saúde digital, interoperabilidade, segurança da informação, governança de dados e uso responsável de inteligência artificial. Sem tais condições, mesmo uma arquitetura tecnicamente adequada pode produzir assimetrias regionais, baixa adesão, fragilidade operacional e dependência excessiva de fornecedores externos.

### 3. Referências

1. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709compilado.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709compilado.htm) Acesso em: 27 maio 2026.
2. BRASIL. **Decreto nº 12.069, de 21 de junho de 2024.** Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital — Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027. Brasília, DF: Presidência da República, 2024. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2024/decreto/d12069.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12069.htm) . Acesso em: 27 maio 2026.
3. BRASIL. **Decreto nº 12.198, de 24 de setembro de 2024.** Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados — IND. Brasília, DF: Presidência da República, 2024. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2024/decreto/d12198.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12198.htm) . Acesso em: 27 maio 2026.
4. G20. **G20 Maceió Ministerial Declaration on Digital Inclusion for All.** Maceió: G20 Digital Economy Working Group, 2024. Disponível em: [https://g7g20-documents.org/fileadmin/G7G20\\_documents/2024/G20/Brazil/Sherpa-Track/Digital%20Economy%20Ministers/1%20Ministers%20Language/G20\\_DEWG\\_Maceio\\_Ministerial\\_Declaration\\_13092024.pdf](https://g7g20-documents.org/fileadmin/G7G20_documents/2024/G20/Brazil/Sherpa-Track/Digital%20Economy%20Ministers/1%20Ministers%20Language/G20_DEWG_Maceio_Ministerial_Declaration_13092024.pdf) . Acesso em: 27 maio 2026.
5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Artificial Intelligence Risk Management Framework (AI RMF 1.0).** Gaithersburg: NIST, 2023. Disponível em: <https://www.nist.gov/itl/ai-risk-management-framework>. Acesso em: 27 maio 2026.
6. WORLD HEALTH ORGANIZATION. **Regulatory considerations on artificial intelligence for health.** Geneva: World Health Organization, 2023. Disponível em: <https://www.who.int/publications/i/item/9789240078871> . Acesso em: 27 maio 2026.

7. NATIONAL AUDIT OFFICE. **The National Programme for IT in the NHS: an update on the delivery of detailed care records systems.** London: National Audit Office, 2011. Disponível em: <https://www.nao.org.uk/reports/the-national-programme-for-it-in-the-nhs-an-update-on-the-delivery-of-detailed-care-records-systems/> . Acesso em: 27 maio 2026.
8. HOUSE OF COMMONS. COMMITTEE OF PUBLIC ACCOUNTS. **The dismantled National Programme for IT in the NHS.** Nineteenth Report of Session 2013–14. London: The Stationery Office, 2013. Disponível em: <https://publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/294/294.pdf>. Acesso em: 27 maio 2026.
9. JUSTINIA, Taghreed. **The UK’s National Programme for IT: why was it dismantled?** *Health Services Management Research*, v. 30, n. 1, p. 2–9, 2017. Disponível em: <https://journals.sagepub.com/doi/10.1177/0951484816662492> Acesso em: 27 maio 2026
10. STERCKX, Sigrid; RAKIC, Vojin; COCKBAIN, Julian; BORRY, Pascal. **“You hoped we would sleep walk into accepting the collection of our data”: controversies surrounding the UK care.data scheme and their wider relevance for biomedical research.** *Medicine, Health Care and Philosophy*, v. 19, n. 2, p. 177–190, 2016. Disponível em: <https://link.springer.com/article/10.1007/s11019-015-9661-6> Acesso em: 27 maio 2026
11. CALDICOTT, Fiona. **Review of data security, consent and opt-outs.** London: National Data Guardian for Health and Care, 2016. Disponível em: <https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs> . Acesso em: 27 maio 2026.
12. CARTER, Pam; LAURIE, Graeme T.; DIXON-WOODS, Mary. **The social licence for research: why care.data ran into trouble.** *Journal of Medical Ethics*, v. 41, n. 5, p. 404–409, 2015. DOI: 10.1136/medethics-2014-102374. Disponível em: <https://pmc.ncbi.nlm.nih.gov/articles/PMC4431337/> Acesso em: 27 maio 2026.
13. CANADA HEALTH INFOWAY. **Vision & Mission.** Toronto: Canada Health Infoway, [s.d.]. Disponível em: <https://www.infoway-inforoute.ca/en/who-we-are/vision-mission> . Acesso em: 27 maio 2026.
14. CANADA HEALTH INFOWAY. **Governance & Accountability.** Toronto: Canada Health Infoway, [s.d.]. Disponível em: <https://www.infoway-inforoute.ca/en/who-we-are/governance-accountability> . Acesso em: 27 maio 2026.
15. CANADA HEALTH INFOWAY. **Digital Health Interoperability Task Force Report.** Toronto: Canada Health Infoway, 2024. Disponível em: <https://www.infoway-inforoute.ca/en/component/edocman/resources/interoperability/6498-digital-health-interoperability-task-force-report> . Acesso em: 27 maio 2026.
16. El Sabawy D, Feldman J, Pinto AD. **The Connected Care for Canadians Act: an important step toward interoperability of health data.** *CMAJ*. 2024 Dec 8;196(42):E1385-E1388. doi: 10.1503/cmaj.241123. PMID: 39653400; PMCID: PMC11627560. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/39653400/> Acesso em: 27 de maio de 2026.
17. AUSTRALIA. **Intergovernmental Agreement on National Digital Health 2023–2027.** Canberra: Australian Government, 2023. Disponível em: <https://federation.gov.au/about/agreements/intergovernmental-agreement-national-digital-health-2023-2027> Acesso em: 27 maio 2026.

18. AUSTRALIAN DIGITAL HEALTH AGENCY. **Annual Report 2019–20**. Sydney: Australian Digital Health Agency, 2020. Disponível em: <https://www.transparency.gov.au/publications/health/australian-digital-health-agency/australian-digital-health-agency-annual-report-2019-20> . Acesso em: 27 maio 2026.
19. MEDCOM. **We are the international gateway to healthcare and life science in Denmark**. Odense: MedCom, [s.d.]. Disponível em: <https://healthcaredenmark.dk/>. Acesso em: 27 maio 2026.
20. EUROPEAN HEALTH TELEMATICS ASSOCIATION. **eHealth Governance: Country Report Denmark**. Brussels: EHTEL, 2021. Disponível em: <https://ehotel.eu/component/attachments/?task=download&id=768:Country-report---Denmark> . Acesso em: 27 maio 2026.
21. METSALLIK, Janek; ROSS, Peeter; DRAHEIM, Dirk; PIHO, Gunnar. **Ten years of the e-health system in Estonia**. In: INTERNATIONAL WORKSHOP ON (META)MODELLING FOR HEALTHCARE SYSTEMS, 3., 2018, Bergen. *CEUR Workshop Proceedings*, v. 2336, p. 6–15, 2018. Disponível em: [https://ceur-ws.org/Vol-2336/MMHS2018\\_invited.pdf](https://ceur-ws.org/Vol-2336/MMHS2018_invited.pdf) . Acesso em: 27 maio 2026.
22. DIGITAL PUBLIC GOODS ALLIANCE. **X-Road® DPG Profile**. Digital Public Goods Registry, 2020. Disponível em: <https://www.digitalpublicgoods.net/r/x-road> . Acesso em: 27 maio 2026.
23. INERA AB. **Inera**. Stockholm: Inera AB, [s.d.]. Disponível em: <https://www.inera.se/> . Acesso em: 27 maio 2026.
24. BÄRKÅS, Annika; SCANDURRA, Isabella; REXHEPI, Hanife; BLEASE, Charlotte; CAJANDER, Åsa; HÄGGLUND, Maria. **Patients’ access to their psychiatric notes: current policies and practices in Sweden**. *International Journal of Environmental Research and Public Health*, v. 18, n. 17, art. 9140, 2021. DOI: 10.3390/ijerph18179140. Disponível em: <https://europepmc.org/article/MED/34501730> Acesso em: 27 de maio de 2026
25. OFFICE OF THE DATA PROTECTION OMBUDSMAN OF FINLAND. **Health care: frequently asked questions**. Helsinki: Office of the Data Protection Ombudsman, [s.d.]. Disponível em: <https://tietosuoja.fi/en/faq-health-care> . Acesso em: 27 de maio 2026.
26. FINDATA. **Legislation**. Helsinki: Finnish Social and Health Data Permit Authority Findata, [s.d.]. Disponível em: <https://findata.fi/en/services-and-instructions/legislation/> . Acesso em: 27 de maio 2026.
27. MOLL, Jonas; REXHEPI, Hanife; CAJANDER, Åsa; GRÜNLOH, Christiane; HUVILA, Isto; HÄGGLUND, Maria; MYRETEG, Gunilla; SCANDURRA, Isabella; ÅHLFELDT, Rose-Mharie. **Patients’ experiences of accessing their electronic health records: national patient survey in Sweden**. *Journal of Medical Internet Research*, v. 20, n. 11, e278, 2018. DOI: 10.2196/jmir.9492. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/30389647/> Acesso em: 27 de maio de 2026
28. HÄGGLUND, Maria; SCANDURRA, Isabella. **User evaluation of the Swedish patient accessible electronic health record: System Usability Scale**. *JMIR Human Factors*, v. 8, n. 3, e24927, 2021. DOI: 10.2196/24927. Disponível em: <https://humanfactors.jmir.org/2021/3/e24927/> Acesso em 27 de maio de 2026.
29. STICHTING MEDMIJ. **Organisation**. The Hague: Stichting MedMij, [s.d.]. Disponível em: <https://medmij.nl/en/organisation/> . Acesso em: 27 de maio 2026.
30. STICHTING MEDMIJ. **MedMij Framework**. The Hague: Stichting MedMij, [s.d.]. Disponível em: <https://medmij.nl/en/medmij-framework/> . Acesso em: 27 maio 2026.

31. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Towards an integrated health information system in the Netherlands**. Paris: OECD Publishing, 2022. Disponível em: [https://www.oecd.org/en/publications/towards-an-integrated-health-information-system-in-the-netherlands\\_a1568975-en.html](https://www.oecd.org/en/publications/towards-an-integrated-health-information-system-in-the-netherlands_a1568975-en.html) . Acesso em: 27 de maio 2026.
32. SANKRITIK, Abhishek; SHETTY, Siddharth. **Digital Public Infrastructure: setting standards with the hourglass model**. Background paper for the *World Development Report 2025: Standards for Development*. Washington, DC: World Bank, 2025. Disponível em: <https://thedocs.worldbank.org/en/doc/5fdabc4891d5c9f0942f7e0f86a72e05-0050062025/original/Abhishek-Sankritik-Digital-public-infrastructure.pdf> . Acesso em: 27 de maio 2026.