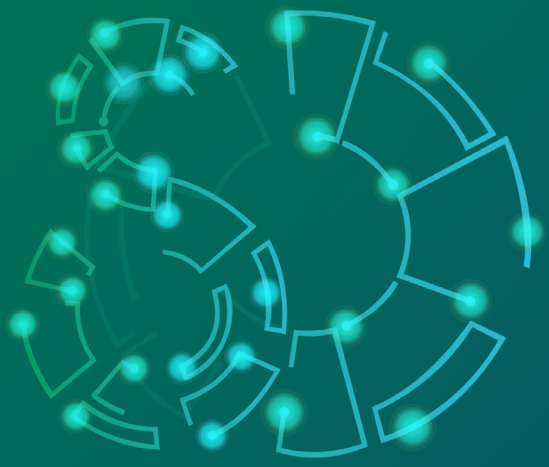


PROGRAMA EDUCACIONAL EM SAÚDE DIGITAL DA UNIVERSIDADE FEDERAL DE GOIÁS

EDUCAÇÃO E CAPACITAÇÃO DE RECURSOS HUMANOS EM SAÚDE DIGITAL

Segurança e ética no compartilhamento de dados pessoais de saúde

Organizadores

Ana Laura de Sene Amâncio Zara
Fábio Nogueira de Lucena
Rejane Faria Ribeiro-Rotta
Renata Dutra Braga
Rita Goreti Amaral
Sheila Mara Pedrosa
Silvana de Lima Vieira dos Santos
Taciana Novo Kudo

Cegraf UFG

DISTRIBUIÇÃO GRATUITA VENDA PROIBIDA

Universidade Federal de Goiás

Reitor

Edward Madureira Brasil

Vice-Reitora

Sandramara Matias Chaves

Diretora do Cegraf UFG

Maria Lucia Kons

Conselho Editorial da Coleção Programa Educacional em Saúde Digital

Ana Laura de Sene Amâncio Zara (IPTSP / Universidade Federal de Goiás)

Fábio Nogueira de Lucena (INF / Universidade Federal de Goiás)

Gabriella Nunes Neves (CGISD / DATASUS / Secretaria Executiva / Ministério da Saúde)

Jacson Venancio de Barros (DATASUS / Secretaria Executiva / Ministério da Saúde)

Juliana Pereira de Souza Zinader (CGISD / DATASUS / Secretaria Executiva / Ministério da Saúde)

Maria Cristina Ferreira de Abreu (CGISD / DATASUS / Secretaria Executiva / Ministério da Saúde)

Rejane Faria Ribeiro-Rotta (FO / Universidade Federal de Goiás)

Renata Dutra Braga (INF / Universidade Federal de Goiás)

Rita Goreti Amaral (FF / Universidade Federal de Goiás)

Sheila Mara Pedrosa (UniEVANGÉLICA)

Silvana de Lima Vieira dos Santos (FEN / Universidade Federal de Goiás)

Taciana Novo Kudo (INF / Universidade Federal de Goiás)

Thais Lucena de Oliveira (CGISD / DATASUS / Secretaria Executiva / Ministério da Saúde)

Equipe de Produção

Amanda Souza Vitor - graduanda (UFG)

Gabriela Martins de Souza - graduanda (UFG)

Iuri Vaz Miranda - graduando (UFG)

Jan Eduardo Macedo Barbosa Junior - graduando (UFG)

Jéssica Borges de Carvalho - técnica-administrativa (UFG)

Luma Wanderley de Oliveira - doutoranda (UFG)

Patrícia Galúcio Coqueiro Galvão - técnica-administrativa (UFG)

Rogério Mendes Vieira - mestrando (UFG)

Virgínia de Fernandes Souza - graduanda (UFG)

Sumaya Jorge Rabelo - graduanda (UFG)

Suse Barbosa Castilho - mestranda (UFG)

Warllson Jesus dos Santos - graduando (UNICEPLAC)

Weverton Ferreira Rodrigues - graduando (UFG)

Comissão de Governança da Informação em Saúde (CGIS)

Silvana de Lima Vieira dos Santos

Centro de Inovação em Gestão da Educação e do Trabalho em Saúde (CIGETS) e Laboratório de Pesquisa em Empreendedorismo e Inovação (LAPEI)

Cândido Vieira Borges Júnior

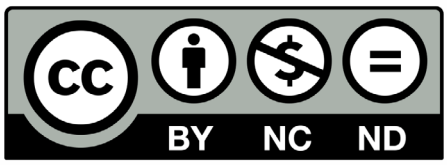
Laboratório de Inovação e Estratégia em Governo (LineGov)

Antônio Isidro da Silva Filho

Ministério da Saúde / Secretaria Executiva / Departamento de Informática do Sistema Único de Saúde (DATASUS)

Jacson Venancio de Barros

Esta obra é disponibilizada nos termos da Licença Creative Commons – Atribuição – Não Comercial – Compartilhamento pela mesma licença 4.0 Internacional. É permitida a reprodução parcial ou total desta obra, desde que citada a fonte



Segurança e ética no compartilhamento de dados pessoais de saúde

Ana Laura de Sene Amâncio Zara
Fábio Nogueira de Lucena
Rejane Faria Ribeiro-Rotta
Renata Dutra Braga
Rita Goreti Amaral
Sheila Mara Pedrosa
Silvana de Lima Vieira dos Santos
Taciana Novo Kudo
(Organizadores)

Cegraf UFG

2021

© Cegraf UFG, 2021

© Ana Laura de Sene Amâncio Zara; Fábio Nogueira de Lucena;
Rejane Faria Ribeiro-Rotta; Renata Dutra Braga; Rita Goreti Amaral;
Sheila Mara Pedrosa; Silvana de Lima Vieira dos Santos; Taciana Novo Kudo, 2021

© Universidade Federal de Goiás, 2021

© Ministério da Saúde, 2021

Revisão editorial
Ana Laura Sene Amâncio Zara

Revisão técnica
Ana Claudia Sayeg Freire Murahovschi (Ministério da Saúde)
Ana Paula de Andrade Pannuti (Ministério da Saúde)
Andréia Cristina de Souza Santos (Ministério da Saúde)
Gabriella Nunes Neves (Ministério da Saúde)
Josélio Emar de Araújo Queiroz (Ministério da Saúde)
Juliana Pereira de Souza Zinader (Ministério da Saúde)
Mara Lucia dos Santos Costa (Ministério da Saúde)
Marcia Elizabeth Marinho da Silva (Ministério da Saúde)
Maria Cristina Ferreira de Abreu (Ministério da Saúde)
Michael Luiz Diana de Oliveira (Ministério da Saúde)
Patricia dos Santos Irigaray Rodrigues (Ministério da Saúde)
Thais Lucena de Oliveira (Ministério da Saúde)

Capa
Iuri Vaz Miranda - graduando (UFG)

Editoração Eletrônica
Luma Wanderley de Oliveira - doutoranda (UFG)
Warllson Jesus dos Santos - graduando (UNICEPLAC)

https://doi.org/10.5216/SEG.ebook.978-85-495-0360-2/2021

Dados Internacionais de Catalogação na Publicação (CIP)
GPT/BC/UFG

S456 Segurança e ética no compartilhamento de dados pessoais de saúde [E-book] / organizadores, Ana Laura de Sene Amâncio Zara ... [et al.]. - Goiânia : Cegraf UFG, 2021.
55 p. : il.

Inclui referências.
ISBN (E-book): 978-85-495-0360-2

1. Proteção de dados - Legislação. 2. Direito e ética - Saúde. 3. Banco de dados - Medidas de segurança. I. Zara, Ana Laura de Sene Amâncio.

CDU: 614:342.7

Bibliotecária responsável: Adriana Pereira de Aguiar / CRB1: 3172

Segurança e ética no compartilhamento de dados pessoais de saúde

Instituição responsável

Universidade Federal de Goiás (UFG)

- Comissão de Governança da Informação em Saúde da UFG (CGIS-UFG)
- Centro de Inovação em Gestão da Educação e do Trabalho em Saúde (CIGETS)
- Laboratório de Pesquisa em Empreendedorismo e Inovação da Universidade Federal de Goiás (LAPEI-UFG)

Instituição financiadora

Ministério da Saúde (MS)

- Secretaria Executiva (SE)
  - Departamento de Informática do Sistema Único de Saúde (DATASUS)
- Secretaria de Gestão do Trabalho e da Educação na Saúde (SGTES)

Apoio

Ministério da Saúde (MS):

- Secretaria de Atenção Primária à Saúde (SAPS)

Demais parceiros

Laboratório de Inovação e Estratégia em Governo (LineGov)

Abreviaturas e Siglas

ACS	Agente Comunitário de Saúde
AISA	Assessoria Internacional
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
ASCOM	Assessoria de Comunicação
Cacon	Centro de Complexidade em Oncologia
CadSUS	Sistema de Cadastramento de Usuários do SUS
CBO	Classificação Brasileira de Ocupações
CDC	Código de Defesa do Consumidor
CGIS	Comissão de Governança da Informação em Saúde
CIGETS	Centro de Inovação em Gestão da Educação e do Trabalho em Saúde
CNES	Cadastro Nacional dos Estabelecimentos de Saúde
CNS	Conselho Nacional de Saúde
CONFEF	Conselho Federal de Educação Física
covid-19	Corona Virus Disease 19 (Doença do Coronavírus)
CPF	Cadastro de Pessoa Física
CREF	Conselhos Regionais de Educação Física
DataSUS	Departamento de Informática do Sistema Único de Saúde do Brasil
Ebserh	Empresa Brasileira de Serviços Hospitalares
ECA	Estatuto da Criança e do Adolescente
ePING	Padrões de Interoperabilidade de Governo Eletrônico
eSF	Equipe de Saúde da Família
e-SUS AB	e-SUS Atenção Básica
ESF	Estratégia Saúde da Família
GAL	Gerenciador de Ambiente Laboratorial
GDPR	*General Data Protection Regulation* - Regulamento Geral de Proteção de Dados
IBGE	Instituto Brasileiro de Geografia e Estatística
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
LAPEI	Laboratório de Pesquisa em Empreendedorismo e Inovação
LGPD	Lei Geral de Proteção de Dados Pessoais
LineGov	Laboratório de Inovação e Estratégia em Governo

Abreviaturas e Siglas

MS	Ministério da Saúde
PEP	Prontuário Eletrônico do Paciente
PNSI	Política Nacional de Segurança da Informação
RAS	Rede de Atenção à Saúde
RNDS	Rede Nacional de Dados em Saúde
RPG	*Role-playing game* - Jogo de interpretação de papéis
SAPS	Secretaria de Atenção Primária à Saúde
SERPRO	Serviço Federal de Processamento de Dados
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SUS	Sistema Único de Saúde
TIC	Tecnologias da Informação e Comunicação
UBS	Unidade Básica de Saúde
UE	União Europeia
UFG	Universidade Federal de Goiás
UNA-SUS	Universidade Aberta do Sistema Único de Saúde
UnB	Universidade de Brasília

Lista de Figuras

Figura 1 - Principais pontos da Lei Geral de Proteção de Dados 17

Vídeo 1 - Entrevista que aborda os aspectos de segurança para compartilhamento acesso à história clínica do cidadão, via Rede Nacional de Dados em Saúde 30

Vídeo 2 - Podcast que discute, na visão da cidadã brasileira Ana, os aspectos de segurança para compartilhamento e acesso à sua história clínica, a partir da RNDS 36

Sumário

Apresentação 11

Unidade 1: Conceitos Importantes 12
1.1 História e Conceitos para o Entendimento da LGPD 13
1.1.1 Histórico 13
1.1.2 LGPD: objetivos, princípios e aspectos éticos 15
1.1.3 Conceitos importantes (LGPD) 18
1.2 Conceitos Importantes para o Acesso Seguro e Ético dos Dados Pessoais a Partir da RNDS 21
1.2.1 Ética profissional 22
1.2.2 A RNDS em conformidade com a LGPD 28
1.3 Entrevista 30

Unidade 2: Orientações para Acesso e Compartilhamento de Dados Pessoais de Saúde 31
2.1 Orientações para Acesso e Compartilhamento de Dados Pessoais de Saúde 32
2.1.1 Contexto 32
2.1.2 Como funciona o compartilhamento dos dados de saúde? 33
2.1.3 Quais Dados Serão Acessados? 33
2.1.4 Por quem e como seus dados de saúde serão acessados? 33
2.1.5 Benefícios 34
2.1.6 Segurança da informação 34
2.1.7 Gestão da base de dados da RNDS 35
2.1.8 E se o cidadão optar por não compartilhar seus dados de saúde? 35
2.1.9 Canais de atendimento 35
2.2 Análise de Situação-problema que Aborda a Segurança e Ética no Compartilhamento de Dados em Saúde 35

Unidade 3: Estratégias para Engajamento e Conscientização do Profissional e do Cidadão 44
3.1 Dicas e Orientações para os Profissionais e Gestores 45
3.2 Dicas e Orientações para os Cidadãos 45
3.3 Jogo Sério 46

Unidade 4: Encerramento do Microcurso 3 47

Referências 49

Apresentação

Prezado(a) Participante,

Seja bem-vindo(a) ao Microcurso 3: **Segurança e ética no compartilhamento de dados pessoais de saúde!**

A sua oferta foi motivada pela necessidade de sensibilizar e preparar os profissionais e gestores do sistema de saúde brasileiro para a implementação da Saúde Digital no Brasil, focada no compartilhamento, segurança, privacidade e confidencialidade de dados pessoais de saúde por meio da Rede Nacional de Dados em Saúde (RNDS).

Este Microcurso apresenta os principais conceitos sobre a segurança e ética; orientações para acesso e compartilhamento de dados pessoais, com atenção à Lei Geral de Proteção de Dados Pessoais (LGPD); e algumas estratégias para engajamento e conscientização de profissionais sobre a gestão do compartilhamento e acesso à história clínica do cidadão, a partir da RNDS.

Esperamos que você sinta-se instigado a conhecer a temática e em colaborar para o fortalecimento do sistema de saúde brasileiro para que seja, cada vez mais, seguro e transparente para profissionais da saúde e usuários do Sistema Único de Saúde (SUS) do Brasil.

Bom estudo!!!

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM **SAÚDE DIGITAL**

Segurança e ética no compartilhamento de dados pessoais de saúde

Unidade 1
Conceitos Importantes

Ana Carolina Figueiredo Modesto,
Ana Laura de Sene Amâncio Zara,
Rejane Faria Ribeiro-Rotta,
Renata Dutra Braga,
Sheila Mara Pedrosa,
Silvana de Lima Vieira dos Santos



Unidade 1: Conceitos Importantes

1.1 História e Conceitos para o Entendimento da LGPD

1.1.1 Histórico

Você sabia que seus dados pessoais se tornaram um bem extremamente precioso? E que muitas instituições públicas e privadas estão de olho neles? As pessoas e instituições estão procurando, cada vez mais, ter o controle sobre os seus dados, pois, os dados pessoais ganharam grande importância na economia moderna, uma vez que permitem fazer predições, analisar perfis de consumo, conhecer opiniões, entre outras atividades. Assim, as empresas podem se beneficiar de alguma forma, por exemplo, ao ter acesso ao seu e-mail para divulgação e venda de produtos, ao saber sobre a sua condição de saúde de forma que seja um(a) potencial consumidor(a) de medicamentos, ao conhecer sua localização geográfica para ofertar propagandas específicas locais, entre tantas outras situações[1].

Então, você concorda que esses dados precisam de proteção e cuidado? Por isso, a preservação de dados privados se tornou um compromisso inadiável, tanto do cidadão, quanto das instituições públicas e privadas que usam esses dados de alguma forma. Essa necessidade de proteção se tornou uma tendência mundial. Atualmente, mais de 126 países possuem leis que regulamentam a proteção de dados pessoais, evitando-se o mau uso desses, bem como a responsabilização em caso de incidentes e acidentes com dados pessoais[2].

A primeira lei oficialmente criada para proteção de dados foi implementada na Alemanha, em 1978. Naquele mesmo ano, França, Noruega, Suécia e Áustria também seguiram essa tendência e sancionaram leis que definiam como as informações de seus cidadãos poderiam ser utilizadas e exportadas. Em 1981, os países membro do Conselho Europeu ajudaram a unificar e desenvolver melhor as normas para o tratamento automatizado de dados pessoais. Em 1995, o Parlamento Europeu e o Conselho da União Europeia (UE) criaram um regulamento que estabelecia regras para serem cumpridas por todos os países da UE, sendo as principais normas relacionadas ao recolhimento de dados de acordo com uma finalidade específica, ao direito ao acesso dos dados por parte do consumidor e à responsabilidade das empresas sobre a segurança das informações armazenadas. Esse regulamento ainda determinava que cada país membro tivesse um órgão ou profissional responsável pela supervisão, implementação e adequação das suas leis regionais[3].

Em 2016, a Comissão Europeia, em acordo com os Estados Unidos, aprovou o Privacy Shieldv, um programa de transferência internacional de dados com empresas norte-americanas que garantia maior segurança para os cidadãos europeus. Após sucessivos episódios de grandes vazamentos de dados, a utilização e comércio de informações pessoais, a UE decidiu rever suas regras de proteção de dados. Então, em 2018, aprovou o General Data Protection Regulation (GDPR) que obrigou empresas de todo mundo – inclusive gigantes como o Facebook® e o Google® – a modificar o modo de coletar e tratar os dados e foi responsável por uma nova onda de novas leis relacionadas ao tema em todo o mundo, o que influenciou fortemente a legislação brasileira[3].

Aqui no Brasil, a história de proteção dos dados iniciou-se com a promulgação da Constituição Federal[4], em 1988, onde no art. 5º refere-se aos direitos e deveres dos cidadãos e trata, ainda que de forma geral, da privacidade dos brasileiros:

> são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação[4].

Em 1993, o Código de Defesa do Consumidor (CDC) evoluiu na busca por proteção de dados e definiu uma seção específica sobre cadastros e bancos de dados pessoais. O cidadão passou a ter o direito de acessar seus dados armazenados pelas empresas e solicitar correção, se necessária. O não cumprimento pelas empresas dessas regras passou a ser considerado infração. No CDC, ainda está prevista a garantia de privacidade e responsabilização das empresas sobre segurança dos dados, que devem ser "preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento"[3].

Em 24 de julho de 1996, a Lei nº 9.296 foi sancionada para regulamentar a interceptação do fluxo de comunicações em sistemas de informática e telemática, acrescentando ao art. 5º da Constituição Federal[4] que

> torna-se inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal[5].

Para assegurar o direito fundamental de acesso à informação previsto na Constituição Federal de 1988[4], foi sancionada a Lei nº 12.527[6], em 18 de novembro de 2011, denominada Lei de Acesso à Informação, que determina que não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais, ou seja, qualquer cidadão pode solicitar informações aos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público.

Em 2013, a primeira lei responsável por regular o uso da Internet no Brasil foi promulgada, denominada Marco Civil da Internet[7], que estabelece princípios, garantias, direitos e deveres para o uso da Internet no País. Ainda em 2013, algumas orientações, que complementam o CDC, foram acrescentadas no Decreto nº 7.962[8], o qual dispõe sobre a contratação do comércio eletrônico definindo que são diretrizes do Plano Nacional de Consumo e Cidadania a

> autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou coletados, inclusive por meio eletrônico[8].

Até então, as leis eram segmentadas, específicas para determinados setores e, principalmente, para as relações comerciais. Até que, em 14 de agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados Pessoais (nº 13.709[9]).

A LGPD é a mudança mais importante no que se refere à privacidade de dados no Brasil, com um conteúdo que pode gerar impactos positivos na vida de milhões de brasileiros e brasileiras. A LGPD surge, assim como a GDPR, da constatação de que os dados pessoais são um ativo econômico valioso, um dado político perigoso e um bem jurídico importante a ser tutelado pela legislação[9].

A fiscalização e a regulação da LGPD ficarão a cargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), cuja criação está prevista na própria LGPD. A ANPD, criada em 2020, é um órgão diretamente ligado à presidência da república, e dentre as diversas competências, destaca-se a obrigatoriedade de zelar pela proteção dos dados dos indivíduos nos termos da LGPD. Em suma, pode-se dizer que a ANPD é o órgão central de interpretação da LGPD no território brasileiro[1].

Vamos conhecer a LGPD para entendermos qual será o seu impacto, de fato, na vida das pessoas?

1.1.2 LGPD: objetivos, princípios e aspectos éticos

A LGPD

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[9].

Para isso, ela é pautada nos seguintes fundamentos[1]:

- **o respeito à privacidade**, ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada;
- **a autodeterminação informativa**, ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos;
- **a liberdade de expressão, de informação, de comunicação e de opinião**, que são direitos previstos na Constituição brasileira;
- **o desenvolvimento econômico e tecnológico e a inovação**, a partir da criação de um cenário de segurança jurídica em todo o país;
- **a livre iniciativa, a livre concorrência e a defesa do consumidor**, por meio de regras claras e válidas para todo o setor privado;
- **os direitos humanos,** o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas.

A LGPD é válida para[1]:

- dados relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento da coleta;
- dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados;
- dados usados para fornecimento de bens ou serviços.

Mas, existem exceções. Nem todos os dados serão tratados de acordo com as diretrizes da LGPD. Por isso, a LGPD não se aplica para fins, exclusivamente[1]:

- jornalísticos e artísticos;
- de segurança pública;
- de defesa nacional;
- de segurança do Estado;
- de investigação e repressão de infrações penais;
- particulares (ou seja, a lei só se aplica para pessoa física ou jurídica que gerencie bases com fins ditos econômicos).
- dados de fora do Brasil e que não sejam objeto de transferência internacional.

A LGPD prevê, ainda, que o tratamento dos dados pessoais do cidadão deve ser pautado em 10 princípios, que são eles[1]:

1. Finalidade especificada e informada explicitamente ao titular;

2. Adequação à finalidade previamente acordada e divulgada;

3. Necessidade do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial;

4. Acesso livre, fácil e gratuito das pessoas à forma como seus dados são tratados.

5. Qualidade dos dados, deixando-os exatos e atualizados, segundo a real necessidade no tratamento.

6. Transparência, ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis;

7. Segurança para coibir situações acidentais ou ilícitas como invasão, destruição, perda e difusão;

8. Prevenção contra danos ao titular e a demais envolvidos;

9. Não discriminação, ou seja, não permitir atos ilícitos ou abusivos. Exemplo: informações sobre diagnósticos de doenças estigmatizadas (aids, transtornos mentais, doenças que impactam no trabalho e que podem prejudicar o emprego), dados de violência doméstica, sexual, dentre outras.

10. Responsabilização do agente, obrigado a demonstrar a eficácia das medidas adotadas[1].

Uma das principais transformações que a LGPD traz para o País é o **consentimento** do cidadão, que se tornou a base para que dados pessoais possam ser tratados. Mas, há algumas situações nas quais é dispensado o consentimento, tais como[1]:



- cumprir uma obrigação legal;
- executar política pública prevista em lei;
- realizar estudos via órgão de pesquisa;
- executar contratos;
- defender direitos em processo;
- preservar a vida e a integridade física de uma pessoa;
- tutelar ações feitas por profissionais das áreas da saúde ou sanitária;
- prevenir fraudes contra o titular;
- proteger o crédito;
- atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

Outra mudança importante que a LGPD promove são as **garantias** concedidas ao cidadão. Por exemplo, ele pode solicitar que os seus dados sejam deletados, pode revogar um consentimento, transferir dados para outro fornecedor de serviços, entre outras ações[1].

Para conhecer mais sobre os principais pontos da LGPD, consulte a Figura 1.

Figura 1 - Principais pontos da Lei Geral de Proteção de Dados Pessoais.

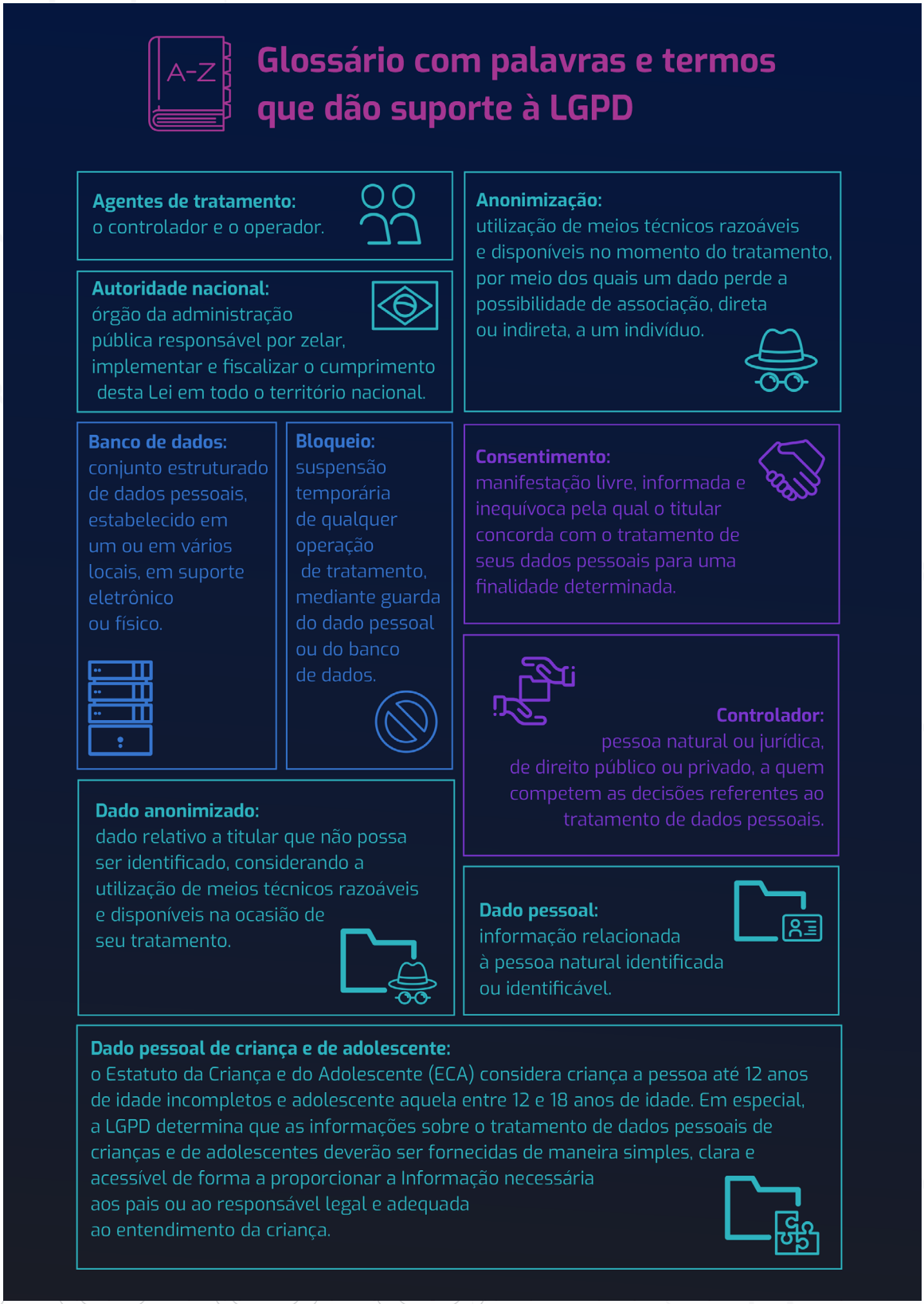


Fonte: SERPRO, 2020[1].

1.1.3 Conceitos importantes (LGPD)

Para entendimento da LGPD[9], vamos conhecer palavras e termos relacionados e o significado de cada um deles?

Com base no glossário, elaborado pelo Serviço Federal de Processamento de Dados (SERPRO)[1], empresa pública de tecnologia da informação, elaboramos o infográfico a seguir, contendo alguns conceitos que dão suporte à LGPD[9].



Dado pessoal sensível:
dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.



Eliminação:
exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.



Encarregado:
pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).



Garantia da segurança da informação:
capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação



Garantia da segurança de dados:
ver garantia da segurança da informação.



Interoperabilidade:
capacidade de sistemas e organizações operarem entre si. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, além dos padrões de interoperabilidade de governo eletrônico (ePING).



Operador:
pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.



Órgão de pesquisa:
órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.



Relatório de impacto à proteção de dados pessoais:
documentação do controlador que contém a descrição dos processos de ratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.



Titular:
pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.



Transferência internacional de dados:
transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.



Tratamento:
toda operação realizada com dados pessoais; como as que se referem a:

acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados

armazenamento - ação ou resultado de manter ou conservar em repositório um dado

arquivamento - ato ou efeito de manter egistrado um dado embora já tenha perdido a validade ou esgotada a sua vigência

avaliação - ato ou efeito de calcular valor sobre um ou mais dados

classificação - maneira de ordenar os dados conforme algum critério estabelecido

coleta - recolhimento de dados com finalidade específica

comunicação - transmitir informações pertinentes a políticas de ação sobre os dados

controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado

difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados

distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido

eliminação - ato ou efeito de excluir ou destruir dado do repositório

extração - ato de copiar ou retirar dados do repositório em que se encontrava

modificação - ato ou efeito de alteração do dado

processamento - ato ou efeito de processar dados

produção - criação de bens e de serviços a partir do tratamento de dados

recepção - ato de receber os dados ao final da transmissão

reprodução - cópia de dado preexistente obtido por meio de qualquer processo

transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro

transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.

utilização - ato ou efeito do aproveitamento dos dados



Uso compartilhado de dados:
comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.



Fonte: Serpro e LGPD (bit.ly/3eELadB)

1.2 Conceitos Importantes para o Acesso Seguro e Ético dos Dados Pessoais a Partir da RNDS

Para garantia do funcionamento da RNDS[10], se faz necessário o esclarecimento de algumas premissas:

- Todos os cidadãos compartilham seus dados de saúde com **profissionais de saúde** para garantia da **continuidade do cuidado**.
- O cidadão, titular de dados pessoais sensíveis de saúde, tem **direito de ser informado** sobre a finalidade e o tratamento de seus dados, portanto, deve ser notificado sempre que algum profissional acessar seus dados.
- O profissional de saúde somente pode acessar os dados de um cidadão durante um **contato assistencial**.
- O contato assistencial pressupõe a **verificação** de três condições: Cadastro de Pessoa Física (CPF) do cidadão, CPF do profissional de saúde e Código Nacional do Estabelecimento de Saúde (CNES) ao qual o profissional é vinculado.

Entende-se por:

- **Cidadão:** usuário dos serviços de atenção à saúde e dos sistemas integrados à RNDS, titular de dados pessoais de saúde.
- **Contato assistencial:** atendimento ininterrupto dispensado a um indivíduo em uma mesma modalidade assistencial e em um mesmo estabelecimento de saúde[11].
- **Continuidade do cuidado:** acompanhamento do paciente ao longo do tempo por profissionais de saúde nos diferentes níveis de atenção à saúde e em diferentes estabelecimentos assistenciais de saúde[12]. A continuidade do cuidado é a finalidade específica para o tratamento de dados na RNDS. Entende-se por tratamento de dados as operações de compartilhamento e acesso de dados pessoais sensíveis referentes à saúde.
- **Compartilhamento e acesso a dados pessoais de saúde:** operações de tratamento de dados que permitem a visualização de dados pessoais sensíveis, referentes à informação de saúde relacionada à pessoa natural identificada e identificável[9].
- **História clínica:** registros de informações geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo[12].

- **Profissionais de Saúde:** profissional da área de saúde subordinado ao correspondente conselho de fiscalização das seguintes categorias profissionais:
    - I - serviço social;
    - II - biologia;
    - III - biomedicina;
    - IV - educação física;
    - V - enfermagem;
    - VI - farmácia;
    - VII - fisioterapia e terapia ocupacional;
    - VIII - fonoaudiologia;
    - IX - medicina;
    - X - medicina veterinária;
    - XI - nutrição;
    - XII - odontologia;
    - XIII - psicologia; e
    - XIV - técnicos em radiologia.

1.2.1 Ética Profissional

Neste escopo agrega-se o papel do profissional sobre o sigilo profissional. Este é compreendido por privacidade[1] de informação[2] e proteção[3] contra revelação[4] não autorizada[12].

Com a RNDS, ao ocorrer o contato assistencial e após a autorização de acesso aos dados correspondentes, o cidadão contará com o sigilo dos profissionais envolvidos na promoção, prevenção, recuperação e reabilitação do estado de saúde desse indivíduo.

Ressalta-se que o profissional de saúde deve estar atento ao que o seu código de ética profissional faz referência sobre a divulgação de informações de saúde do indivíduo. Atentando-se para as suas responsabilidades, proibições e deveres em relação ao **sigilo profissional**, como descrito a seguir:

Ao(À) **Assistente Social** é permitida:

> a revelação, dentro do estritamente necessário, quer em relação ao assunto revelado, quer ao grau e número de pessoas que dele devam tomar conhecimento[13].

[1] Privacidade: e estado de estar livre de intrusão ou perturbação na vida privada de uma pessoa ou em seus negócios.

[2] Informação: comunicação ou recepção de um ou de um conjunto de conhecimentos ou juízos reunidos sobre determinado assunto ou o conjunto desses conhecimentos ou juízos.

[3] Proteção:Ação para garantir segurança e vigilância nas áreas afetadas, bem como ajudar a reduzir a perda de vidas.

[4] Revelação: Revelação de informação por comunicação oral ou escrita.

O(A) **Biólogo(a)** deve:

> Manter a privacidade e confidencialidade de resultados de testes genéticos de paternidade, de doenças e de outros procedimentos (testes/experimentação/pesquisas) que possam implicar em prejuízos morais e sociais ao solicitante, independentemente da técnica utilizada. Parágrafo único: Não será observado o sigilo profissional previsto no caput deste artigo, quando os resultados indicarem riscos ou prejuízos à saúde humana, à biodiversidade e ao meio ambiente, devendo o profissional comunicar os resultados às autoridades competentes[15].

Em relação aos(às) **Biomédicos(as)**:

> são direitos dos mesmos, resguardar o segredo profissional e ter respeitada, em nome da liberdade de profissão e do sigilo profissional, a inviolabilidade de seu laboratório, ou local de trabalho, de seus arquivos e dados, de sua correspondência e de suas comunicações, inclusive telefônicas ou afins, salvo caso de requisição judicial[16].

Quanto aos(às) profissionais de **Educação Física**, esses devem:

> guardar sigilo sobre fato ou informação de que tiver conhecimento em decorrência do exercício da profissão, admitindo-se a exceção somente por determinação judicial ou quando o fato for imprescindível como única forma de defesa perante o Tribunal de Ética do Sistema CONFEF/CREFs[17].

Os(As) profissionais de **Enfermagem** devem:

> manter sigilo sobre fato de que tenha conhecimento em razão da atividade profissional, exceto nos casos previstos na legislação ou por determinação judicial, ou com o consentimento escrito da pessoa envolvida ou de seu representante ou responsável legal[18].

Os(As) **Farmacêuticos(as)** tem como dever:

> guardar sigilo de fatos e informações de que tenha conhecimento no exercício da profissão, excetuando-se os casos amparados pela legislação vigente, cujo dever legal exija comunicação, denúncia ou relato a quem de direito; Não permitir que terceiros tenham acesso a senhas pessoais, sigilosas e intransferíveis, utilizadas em sistemas informatizados e inerentes à sua atividade profissional[19].

Quanto ao(à) **Fisioterapêuta** e ao(à) **Terapêuta ocupacional**, estes profissionais são proibidos de:

> revelar, sem justa causa, fato sigiloso de que tenha conhecimento em razão do exercício de sua profissão;
> Negligenciar na orientação de seus colaboradores, quanto ao sigilo profissional;
> Fazer referência a casos clínicos ou de assistência social identificáveis, exibir cliente/paciente/usuário/família/grupo/comunidade ou sua imagem em anúncios profissionais ou na divulgação de assuntos terapêuticos ocupacionais em qualquer meio de comunicação, salvo quando autorizado pelo cliente/paciente/usuário/família/grupo/comunidade ou seu responsável legal[20].

O(A) **Fonoaudiólogo(a)** deve:

> guardar sigilo sobre as informações de outros profissionais também comprometidos com o caso; Conservar prontuários físicos ou eletrônicos de seus clientes em arquivo apropriado, não permitindo o acesso de pessoas estranhas a este; Orientar seus colaboradores, alunos, estagiários e residentes sob sua orientação, quanto ao sigilo profissional e guarda de prontuário; Manter sigilo sobre as informações e fatos de que tenha conhecimento em decorrência de sua atuação com o cliente, exceto: a) em situações em que o seu silêncio ponha em risco a integridade do profissional, do cliente ou da comunidade, devendo o fato ser comunicado aos órgãos competentes; b) no cumprimento de determinação judicial[21].

É proibido aos(às) **Médicos(as)**:

> revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.
> Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha (nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento); c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal.
> Revelar sigilo profissional relacionado a paciente criança ou adolescente, desde que estes tenham capacidade de discernimento, inclusive a seus pais ou representantes legais, salvo quando a não revelação possa acarretar dano ao paciente.
> Fazer referência a casos clínicos identificáveis, exibir pacientes ou imagens que os tornem reconhecíveis em anúncios profissionais ou na divulgação de assuntos médicos em meios de comunicação em geral, mesmo com autorização do paciente.
> Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.
> Prestar informações a empresas seguradoras sobre as circunstâncias da morte do paciente sob seus cuidados, além das contidas na declaração de óbito, salvo por expresso consentimento do seu representante legal.
> Deixar de orientar seus auxiliares e alunos a respeitar o sigilo profissional e zelar para que seja por eles mantido.
> Deixar de guardar o sigilo profissional na cobrança de honorários por meio judicial ou extrajudicial.[22]

O(A) **Médico(a) Veterinário(a)** não poderá:

fazer referências a casos clínicos identificáveis, exibir pacientes ou suas fotografias em anúncios profissionais ou na divulgação, de assuntos profissionais em programas de rádio, televisão, cinema, na Internet, em artigos, entrevistas, ou reportagens em jornais revistas e outras publicações leigas, ou em quaisquer outros meios de comunicação existentes e que venham a existir, sem autorização expressa do cliente;

Prestar a empresas ou seguradoras, qualquer informação técnica sobre paciente ou cliente sem expressa autorização do responsável legal, exceto nos casos de ato praticado com dolo ou má fé por uma das partes ou quando houver risco à saúde pública, ao meio ambiente ou por força judicial;

Permitir o uso do cadastro de seus clientes sem a respectiva autorização; facilitar o acesso e conhecimento dos prontuários, relatórios e demais documentos sujeitos ao sigilo profissional;

Revelar fatos que prejudiquem pessoas ou entidades sempre que o conhecimento advenha do exercício de sua profissão, ressalvados os atos de crueldade e os interessam ao bem comum, à saúde pública, ao meio ambiente ou que decorram de determinação judicial[23].

É dever do(a) **Nutricionista**:

manter o sigilo e respeitar a confidencialidade de informações no exercício da profissão, salvo em caso de exigência legal, considerando ainda as seguintes situações: impedir o manuseio de quaisquer documentos sujeitos ao sigilo profissional por pessoas não obrigadas ao mesmo compromisso. Caso considere pertinente, o nutricionista poderá fornecer as informações, mediante assinatura de termo de sigilo ou confidencialidade pelo solicitante. Respeitar o direito à individualidade e intimidade da criança e do adolescente, nos termos da legislação vigente, em especial do Estatuto da Criança e do Adolescente, sendo imperativa a comunicação ao seu responsável de situação de risco à saúde ou à vida[24].

Para o(a) **Odontólogo(a)** constitui infração ética:

> revelar, sem justa causa, fato sigiloso de que tenha conhecimento em razão do exercício de sua profissão; negligenciar na orientação de seus colaboradores quanto ao sigilo profissional; e fazer referência a casos clínicos identificáveis, exibir paciente, sua imagem ou qualquer outro elemento que o identifique, em qualquer meio de comunicação ou sob qualquer pretexto, salvo se o cirurgião-dentista estiver no exercício da docência ou em publicações científicas, nos quais, a autorização do paciente ou seu responsável legal, lhe permite a exibição da imagem ou prontuários com finalidade didático-acadêmicas[25].

É dever do **Psicólogo(a)**:

> respeitar o sigilo profissional a fim de proteger, por meio da confidencialidade, a intimidade das pessoas, grupos ou organizações, a que tenha acesso no exercício profissional[26].

Ao(À) profissional **Técnico(a) em Radiologia** constitui infração ética:

> revelar, fato sigiloso de que tenha conhecimento em razão do exercício de sua profissão;
> Negligenciar na orientação de seus colaboradores quanto ao sigilo profissional;
> Fazer referência a casos clínicos identificáveis, exibir clientes ou seus exames e fotografias em anúncios profissionais ou na divulgação de assuntos Radiológicos em programas de rádio, televisão ou cinema, e em artigos, entrevistas ou reportagens em jornais, revistas, congressos, simpósios e aulas ou outras publicações legais, salvo se autorizado pelo cliente/paciente ou responsável.
> Parágrafo único. Compreende-se como justa causa, principalmente: colaboração com a justiça nos casos previstos em Lei; notificação compulsória de doença; perícia radiológica nos seus exatos limites; estrita defesa de interesse legítimo dos profissionais inscritos; revelação de fato sigiloso ao responsável pelo incapaz[27].

Assim, em respeito à legislação, o cidadão contará com a observância dos aspectos ético-legais descritos nos Códigos de Ética dos profissionais de saúde e da Tecnologia da Informação e Comunicação (TIC).

1.2.2 A RNDS em conformidade com a Lei Geral de Proteção de Dados Pessoais

A implementação da RNDS[10] iniciou-se em junho de 2019, com os objetivos de oferecer benefícios de melhoria da assistência à saúde, a partir do acesso às informações e continuidade do cuidado nos níveis de atenção, permitir eficiência na gestão dos recursos públicos e impulsionar a inovação na saúde.

Em março de 2020, a abrangência e o escopo do projeto da RNDS foram direcionados ao enfrentamento da covid-19 (Corona Virus Disease 19), para o fortalecimento da resposta do sistema de saúde, monitoramento e gestão da saúde populacional, oferta de soluções para engajamento ativo do usuário no controle da epidemia e processamento do esperado número de casos da doença[10].

Desde as primeiras ações de planejamento, governança, definição de arquitetura e de regras negociais, o Departamento de Informática do SUS (DATASUS) se prepara para manter a RNDS em conformidade com a LGPD[28].

Apresentam-se abaixo as principais medidas tomadas até o momento[29]:

- Instituição do Núcleo LGPD pela Portaria DATASUS de 22 de novembro de 2019, que visa a adequada implementação das medidas preconizadas na LGPD;
- Elaboração de Relatório de Avaliação de Conformidade pelo Núcleo LGPD e estudo piloto de conformidade com o Sistema de Cadastramento de Usuários do SUS (CadSUS);
- Estudo de Conformidade da RNDS com a LGPD, com destaque para nove aspectos essenciais de análise: Governança de Informação, Definição de Papéis e Responsabilidades, Categorização dos Dados, Segurança da RNDS, Gestão de Continuidades, Tratamento de Dados, Consentimento, Anonimização de Dados, Transparência e Direitos do Titular;
- Início do Projeto "Expansão da RNDS – Iniciativas em LGPD" com *Better Health Program Brazil – Prosperity Fund*, no âmbito da Cooperação Internacional Brasil e Reino Unido, ação desenvolvida em parceria com a Assessoria Internacional (AISA-MS);
- Gerenciamento de Riscos do Programa Conecte SUS, acompanhado pela Diretoria de Integridade; e
- Elaboração de uma nota conjunta com a Assessoria de Comunicação (ASCOM-MS) para elaboração de um Plano de Comunicação que contemple a disponibilização de ampla e adequada informação ao titular de dados quanto aos direitos previstos na LGPD[29].

Quanto aos aspectos de segurança da RNDS, ressalta-se que os dados de saúde serão coletados, processados e armazenados de acordo com padrões de confidencialidade e segurança proporcionais à sua sensibilidade.

O acesso aos dados da RNDS está restrito ao **Titular** (por meio do aplicativo Conecte SUS), mediante autenticação realizada por meio do acesso gov.br[30]; e aos **Profissionais de Saúde** (por meio do Portal Conecte SUS – Perfil Profissional de Saúde), mediante autenticação do Certifica-

ção Digital ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) de instalações de Prontuário Eletrônico do Paciente (PEP) previamente habilitado para o estabelecimento de saúde e restrito ao contexto de atendimento, ou seja, apenas durante o contato assistencial com o indivíduor[31].

Todos os acessos aos dados são rastreados, ou seja, a RNDS é capaz de identificar de forma inequívoca que dado foi acessado, por qual profissional, em que estabelecimento de saúde se deu a consulta e quando (data/hora) essa consulta foi realizada. A RNDS também é capaz de rastrear a origem de todo documento exposto no Portal Conecte SUS.

No aplicativo Conecte SUS, o cidadão (titular de dados) **será sempre notificado quando sua história clínica for acessada pelo profissional de saúde.** Uma lista do histórico de todos os acessos de profissionais de saúde estará disponível para visualização pelo cidadão, no aplicativo Conecte SUS.

É importante salientar que as normativas e diretrizes da própria LGPD ainda estão em fase de construção, discussão e análise de impacto, com destaque à criação da ANPD, prevista na LGPD e a criação do Comitê Central de Governança de Dados, previsto no Decreto N° 10.046, de 9 de outubro de 2019[32].

No entanto, enquanto órgão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), o DATASUS tem participado de discussões e seguido as orientações dispostas no Guia de Boas Práticas da LGPD[33] para implementação na Administração Pública Federal, divulgado pela Secretaria de Governo Digital do Ministério da Economia.

O DATASUS está em fase de preparação para manter a RNDS em conformidade com as diretrizes e regras de tratamento de dados pessoais previstas na LGPD. No entanto, compreende-se que o esforço de aderência à LGPD deva ocorrer de maneira ampliada, com comprometimento e engajamento de vários atores do Ministério da Saúde, de forma contínua, progressiva e transparente.

Dentre as exigências da Lei, destacam-se a institucionalização dos princípios e diretrizes da LGPD no âmbito do SUS, a partir das análise da LGPD com outras bases legais de saúde; a formalização dos papéis e perfis definidos pela Lei, como controlador(es), operador(es) e encarregado(s); definição e finalidade específica para cada tipo de acesso, e por fim, o fortalecimento dos instrumentos de comunicação nos canais de apoio ao titular dos dados.

1.3 Entrevista

Assista no vídeo a seguir a entrevista com a Especialista Jackeline Neves de Almeida, Coordenadora de Segurança da Informação do DataSUS.

Vídeo 1 - Entrevista que aborda os aspectos de segurança para compartilhamento e acesso à história clínica do cidadão, via Rede Nacional de Dados em Saúde.



Fonte: Autoria própria.

Para relembrar...

- Dado pessoal sensível é todo dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Assim, todos os dados de saúde de um cidadão são, portanto, dados sensíveis.
- Como o cidadão ficará sabendo que alguém acessou seus dados de saúde? No Aplicativo Conecte SUS, o cidadão (titular de dados) será sempre notificado quando sua história clínica for acessada por um profissional de saúde. Uma lista do histórico de todos os acessos de profissionais de saúde estará disponível para visualização pelo cidadão, no Aplicativo Conecte SUS.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM **SAÚDE DIGITAL**

Segurança e ética no compartilhamento de dados pessoais de saúde

Unidade 2
Orientações para acesso e compartilhamento de dados pessoais de saúde

Ana Laura de Sene Amâncio Zara,
Rejane Faria Ribeiro-Rotta,
Renata Dutra Braga,
Sheila Mara Pedrosa,
Silvana de Lima Vieira dos Santos,
Suse Barbosa Castilho



Unidade 2: Orientações para acesso e compartilhamento de dados pessoais de saúde

2.1 Orientações para Acesso e Compartilhamento de Dados Pessoais de Saúde

2.1.1 Contexto

Todas as vezes em que o cidadão recebe cuidados de um profissional de saúde registrado, para diagnóstico, tratamento, ou prevenção de uma enfermidade ou orientação sobre sua saúde, seja no sistema de saúde público ou privado, **dados de saúde** desse encontro assistencial são coletados, registrados e armazenados eletronicamente nos sistemas locais de informação.

Esses dados são usados para documentação desse encontro e para comunicação do seu histórico a outros profissionais de saúde que estiverem colaborando para que o cidadão recupere sua saúde totalmente e permaneça saudável. A coleta, o registro e o armazenamento de dados de saúde são etapas muito importantes para garantir que você tenha acesso a ações e serviços de saúde de qualidade, no momento em que você precisa.

Além de agilizar seu atendimento e possibilitar que você receba os cuidados mais adequados para o seu caso, a documentação do seu histórico de saúde serve também para o cumprimento de obrigações éticas, regulatórias e legais por parte de quem lhe presta os cuidados – profissionais e instituições de saúde.

A RNDS, mantida pelo Ministério da Saúde, foi criada para que os dados de saúde possam ser trocados de forma responsável, segura e confidencial, entre os profissionais de saúde que cuidam para que o cidadão receba uma atenção integral e de qualidade, garantindo que as informações essenciais para dar continuidade ao tratamento estejam disponíveis sempre que o cidadão necessitar, mesmo que esteja sendo tratado com profissionais que não trabalham em um mesmo estabelecimento, ou nem no mesmo município, estado ou país. Por meio do armazenamento dos seus dados de saúde na RNDS, o cidadão poderá ter um atendimento de qualidade em qualquer lugar e em qualquer momento.

A LGPD considera os dados de saúde, ou seja, dados referentes à saúde do cidadão, à vida sexual, dado genético ou biométrico, como dados pessoais **sensíveis**. Isso significa que os dados de saúde do cidadão, registrados em meio eletrônico ou físico, devem ser protegidos e tratados com mais atenção, pois, são dados que podem predispor a algum tipo de discriminação. Por isso, na RNDS, todas as atividades que envolvam a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, ou ainda, o compartilhamento dos dados de saúde do cidadão com terceiros, seguirão os princípios e obrigações dispostos na LGPD[9] e demais normas que regulam essas atividades.

Todos os cidadãos usuários do SUS participam da RNDS automaticamente, pois, o País coleta dados de todos os brasileiros e estrangeiros usuários do SUS para conhecer a situação de saúde da população. A RNDS será utilizada para o cumprimento das obrigações com a população brasileira, pois, por meio dos dados de saúde será possível avaliar, formular e executar políticas públicas mais eficazes, estabelecendo condições para promoção, proteção, tratamento e recuperação da sua saúde e da população.

No entanto, neste momento, o cidadão poderá escolher não compartilhar os seus dados de saúde com profissionais de saúde que tenham acesso à RNDS. Ao escolher esta opção, os dados de saúde do cidadão compartilhados com os profissionais de assistência à saúde, responsáveis pelos seus atendimentos, ficarão restritos aos sistemas do Ministério da Saúde e poderão ser compartilhadas de maneira anonimizada. Esta possibilidade poderá ser revista a qualquer momento, ocasião em que o cidadão será devidamente informado a respeito.

2.1.2 Como funciona o compartilhamento dos dados de saúde?

Os dados de saúde do cidadão estarão disponíveis ao profissional de saúde que esteja prestando atendimento ao mesmo ou à pessoa pela qual o cidadão seja responsável legal. Este profissional de saúde deverá estar habilitado a acessar os dados da RNDS, do Ministério da Saúde, por meio de seu cadastro no Conecte SUS Profissional.

2.1.3 Quais dados serão acessados?

O profissional de saúde terá acesso a informações de caráter administrativo (por exemplo, data e horários de atendimento, entrada e saída do estabelecimento), informações relativas a medicamentos distribuídos, internações hospitalares, atendimentos ambulatoriais, de vacinação e resultados de exames.

Ao acessar a RNDS, o profissional de saúde terá acesso somente a dados de saúde coletados a partir de janeiro de 2018.

2.1.4 Por quem e como seus dados de saúde serão acessados?

O profissional de saúde que, no exercício regular de sua profissão, esteja diretamente envolvido nas ações e nos serviços de saúde prestados ao cidadão, estará autorizado a acessar os dados de saúde do mesmo.

2.1.5 Benefícios

O objetivo da RNDS é facilitar o acesso dos **profissionais de saúde** que venham a cuidar do cidadão às informações precisas e atualizadas sobre o seu histórico e condições presentes de saúde. O acesso aos dados de saúde do cidadão poderá estar disponível para esses profissionais no exato momento em que o mesmo precisar (contato assistencial). Isso é muito importante para que possa ser possível prestar um atendimento mais individualizado e direcionado às necessidades do cidadão. Por meio da RNDS, se espera melhorar a comunicação entre todos profissionais que cuidam do cidadão, de modo que eles atuem de forma integrada e contínua para o seu benefício, evitando que o cidadão tenha que repetir exames ou outros procedimentos desnecessariamente. Essa integração contribui, ainda, para que as decisões deles sejam melhor informadas e que o cidadão tenha uma atenção personalizada, segura e mais adequada às suas necessidades.

O cidadão será atendido com muito mais rapidez, qualidade, eficiência e segurança. Afinal, quanto mais o profissional de saúde conhecer sobre o cidadão, seus hábitos e seu histórico de saúde, melhor e mais assertivos poderão ser os cuidados como prevenção, diagnóstico e tratamento, mesmo que esteja atendendo o cidadão pela primeira vez. Outro exemplo: saber, imediatamente, quais medicamentos o cidadão usa ou já usou, se o mesmo tem alergias, quais os resultados dos exames já realizados, assim como ter acesso a relatórios cirúrgicos e notas de internação é muito importante para evitar diagnósticos e tratamentos inadequados ou ineficientes e, como consequência, eventuais prejuízos à saúde do cidadão.

Outra vantagem é que quando estiver em um **atendimento de emergência**, no qual, por exemplo, o cidadão esteja inconsciente e/ou desacompanhado e, portanto, incapaz de fornecer informações sobre seu estado ou histórico de saúde, o profissional de saúde que estiver atendendo o cidadão poderá acessar seus dados de saúde e conhecer a história clínica do mesmo.

2.1.6. Segurança da informação

Os dados de saúde serão coletados, processados e armazenados de acordo com padrões de confidencialidade e segurança proporcionais à sua sensibilidade, o que implica na criação de ambientes físicos e lógicos aderentes ao estado da técnica e às melhores práticas em gestão do sigilo e da segurança da informação, inclusive aqueles específicos à área de saúde.

Embora os estabelecimentos de saúde integrantes da RNDS e a própria RNDS estejam cercados de todos os cuidados voltados ao sigilo e a segurança de seus dados de saúde, é impossível garantir a inviolabilidade de seus sistemas, seja em razão da ocorrência de casos fortuitos, motivos de força maior ou em razão de ataques cibernéticos que possam vir a ocorrer.

Todos os acessos aos dados de saúde do cidadão serão registrados eletronicamente e o mesmo será notificado no Aplicativo Conecte SUS Cidadão sempre que seu registro for acessado. Os acessos não autorizados e usos indevidos por usuários da RNDS estarão sujeitos a penalidades previstas na legislação. É direito do cidadão, a qualquer momento, ter conhecimento dos acessos realizados aos seus dados de saúde.

Caso o cidadão decida não compartilhar seus dados de saúde, os seus atendimentos nos estabelecimentos de saúde não sofrerão qualquer restrição. Nesse caso, o estabelecimento de saúde somente compartilhará os dados de saúde do cidadão com terceiros nas situações exigidas por lei ou pelos códigos e normas de ética médica, por exemplo, ordem judicial, hipóteses

de comunicado compulsório de doenças.

Em casos de atendimento de emergência, em que não haja registro de autorização para compartilhamento dos dados de saúde do cidadão, ou quando o mesmo não estiver em condições de dar esse consentimento, o profissional de saúde responsável pelo seu atendimento poderá acessar seus dados de saúde, nas seguintes situações: (i) a partir de autorização expressa de seu representante legal ou acompanhante; ou (ii) quando, a partir do julgamento técnico do profissional de saúde responsável, o cidadão corra risco de lesão grave ou risco de morte. O acesso aos dados de saúde nessa segunda hipótese deverá ser devidamente justificado e registrado na RNDS para futura auditoria.

2.1.7. Gestão da base de dados da RNDS

A RNDS utiliza uma tecnologia de armazenamento em nuvem, o que permite guardar dados na Internet por meio de um servidor *online*. A aquisição, instalação e manutenção dessa tecnologia, bem como a gestão da base de dados estão sob responsabilidade do DataSUS, do Ministério da Saúde. Caso a gestão da base de dados de saúde seja transferida a terceiros, o cidadão será notificado da ocorrência dessa mudança com a devida antecedência.

As Secretarias de Saúde do Estado e do Município aos quais o estabelecimento de saúde integrante da RNDS estiver vinculado poderão ter acesso a essas informações de forma que o cidadão não poderá ser identificado, ou seja, os dados serão anonimizados.

2.1.8. E se o cidadão optar por não compartilhar seus dados de saúde?

Caso o cidadão decida não compartilhar seus dados de saúde, os seus atendimentos nos estabelecimentos de saúde não sofrerão qualquer restrição. Nesse caso, o estabelecimento de saúde somente compartilhará os dados de saúde do cidadão com terceiros nos casos exigidos por lei ou pelos códigos e normas de ética médica, por exemplo, ordem judicial, hipóteses de comunicado compulsório de doenças.

2.1.9. Canais de atendimento

Sempre que desejar, o cidadão poderá entrar em contato com a equipe da RNDS. Em caso de dúvidas, reclamações ou perguntas sobre os seus direitos, o cidadão poderá entrar em contato no seguinte e-mail: rnds@saude.gov.br.

2.2 Análise de Situação-problema que Aborda a Segurança e Ética no Compartilhamento de Dados

Assista um diálogo, em formato de *podcast*, sobre essa revisita, mais uma vez, ao "Caso de Ana"[34].

Os participantes deste *podcast* foram:

- Representando o profissional de saúde: **Ana Cláudia Cielo**. É nutricionista, com Residência em Saúde da Família, especialista em Gestão de Políticas de Saúde Informadas por Evidências e em Informática em Saúde. É mestre em Políticas Públicas em Saúde (Fiocruz/Brasília) e analista de negócios em saúde na Estratégia e-SUS Atenção Básica (e-SUS AB) na Coordenação Geral de Informação da Atenção Primária, do Departamento de Saúde da Família, da Secretaria de Atenção Primária à Saúde do Ministério da Saúde.
- Representando os profissionais de Tecnologia da Informação: **Lucas Calabrez Pereyra**. É Engenheiro de Computação e mestre em Ciências (Universidade de São Paulo - Ribeirão Preto). Faz parte da equipe da Coordenação-Geral de Sistemas de Informação e Operações no DATASUS.
- Responsável pela narração dos momentos selecionados do Caso de Ana: **Suse Barbosa Castilho**. É enfermeira do Hospital das Clínicas da Universidade Federal de Goiás(UFG)/Ebserh, especialista em Preceptoria pelo SUS e Saúde Pública e membro da equipe de produção do Programa Educacional em Saúde Digital.
- Responsável pela mediação do podcast: **Sheila Mara Pedrosa**. É enfermeira e doutora em Ciências da Saúde pela UFG e conteudista do Programa Educacional em Saúde Digital.

Vídeo 2 - Podcast que discute, na visão da cidadã brasileira Ana, os aspectos de segurança para compartilhamento e acesso à sua história clínica, a partir da RNDS.



Fonte: Autoria própria.

No Microcurso 2, utilizamos o ilustrativo “Caso de Ana”[34] para refletirmos sobre as diversas situações e desafios que se apresentam no processo de organização de uma rede de serviços de saúde que afetam a vida e o destino das pessoas e, na segunda parte, demonstramos os benefícios da RNDS, utilizando as vantagens da saúde digital no processo de diagnóstico e tratamento do do câncer de mama de uma cidadã brasileira.

Retomamos o caso de Ana, mais uma vez, para que você possa entender como será garantida a segurança e confidencialidade dos dados em saúde pela RNDS, em conformidade com a LGPD. O intuito é reforçar a importância do objetivo central da RNDS, que é permitir a troca segura de informações entre os pontos da Rede de Atenção à Saúde (RAS).

ANA TEM SINAL DE ALERTA!

Ana, uma mulher de 53 anos, acordou no sábado apresentando dor, secreção em um mamilo e ao autoexame percebeu um pequeno volume na mama direita.

Sempre muito atenta com a saúde, Ana acessou o aplicativo ConecteSUS pelo seu celular, utilizando o seu CPF. Ela conseguiu solicitar um agendamento com o médico da Unidade Básica de Saúde (UBS), a qual estava vinculada. Foi por meio da equipe dessa UBS que ela ficou sabendo do aplicativo, no qual, após ter baixado no seu celular, se cadastrou via “Meu gov.br”.

Os dados do cadastro pessoal e da história clínica de Ana são sensíveis[1] e, por isso, necessitam de um protocolo de confiança (chamado de *blockchain*[2]) para a criptografia[3] e proteção dos dados, armazenados na nuvem, por meio de um servidor *online*[4].

Ainda na tela do aplicativo Conecte SUS Cidadão, a Ana optou por permitir que os profissionais de saúde, responsáveis pelo seu cuidado, possam acessar e compartilhar seus dados de saúde, via RNDS.

Ana estava na casa da vizinha e foi notificada via celular que o seu atendimento havia sido agendado para segunda-feira. Ana ficou um pouco mais tranquila ao saber que iria consultar com o seu médico da sua equipe de Saúde da Família (eSF).

Na manhã de segunda-feira, Ana chegou na UBS e foi acolhida pela enfermeira sem esperar em fila e teve seu agendamento identificado no sistema.

[1] Dados sensíveis: segundo a LGPD são Dados de Saúde, ou seja, Dados referentes à saúde do cidadão, à vida sexual, dado genético ou biométrico. Podendo ser o cidadão identificado ou discriminado.

[2] Blockchain: solução responsável por tratar questões de segurança, rastreabilidade, desempenho, acesso e escalabilidade (estar preparado para crescer) do software.

A enfermeira, ao acessar o Prontuário Eletrônico do Paciente (PEP) onde atua, que é integrado à RNDS, fez a busca pelo cadastro de Ana informando o seu número de Cadastro de Pessoa Física (CPF) ou do Cartão Nacional de Saúde (CNS). Assim, o PEP, no qual a enfermeira está com acesso autorizado, envia os dados para acesso à RNDS: CPF e Classificação Brasileira de Ocupações (CBO)[6] do profissional de saúde, número do registro do estabelecimento de saúde (CNES), código do município de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), certificado digital, identificação de instalação homologada para integrar à RNDS e o CPF do cidadão que está sendo atendido. A RNDS valida a autorização da instalação e do profissional. Somente com todos esses dados validados, a RNDS disponibiliza a história clínica da Ana no contexto assistencial e, então, a enfermeira tem acesso a esses dados por meio do PEP.

Para todo e qualquer acesso e compartilhamento dos dados da história clínica de Ana, a RNDS enviará uma notificação à cidadã, podendo a mesma visualizar todo o histórico de acessos dos profissionais por meio do Aplicativo Conecte SUS Cidadão.

Ana foi examinada pelo médico da ESF, que acessou o histórico de saúde da mesma e verificou que ela possuía histórico familiar de câncer de mama.

O médico, também está com o acesso autorizado no Conecte SUS Profissional e precisa acompanhar o caso de Ana para garantir um melhor atendimento a ela na RAS. Assim, ele precisa ter responsabilidade e garantir o sigilo e a confidencialidade dos dados, sendo, portanto, um tutor temporário dos dados de Ana, ou seja, estarão disponíveis somente durante o atendimento/contato assistencial.

O município de Ana, por meio de protocolos pré-estabelecidos, permitia que médicos da ESF solicitassem alguns exames específicos. O médico, então, solicitou no sistema de regulação a mamografia e prescreveu analgésico para o caso de dor.

Após uma semana, Ana é notificada que sua mamografia foi agendada para o prazo de oito dias, a ser realizada na Capital.

[6] Classificação Brasileira de Ocupações (CBO): é o documento normalizador do reconhecimento, da nomeação e da codificação dos títulos e conteúdos das ocupações do mercado de trabalho brasileiro.

Nesse momento, dois conceitos principais são evidenciados: a interoperabilidade semântica[7] entre sistemas, onde sistemas de diferentes estabelecimentos de saúde "interpretam" corretamente as informações trocadas, ou seja, a informação tem o mesmo significado entre o sistema receptor e o sistema emissor; e o uso da tecnologia *blockchain* para a proteção, imutabilidade e rastreabilidade dos dados trocados entre a UBS e o laboratório de radiologia, garantindo um registro de transações permanentes e à prova de violações.

Ao realizar a mamografia, Ana foi informada que o resultado seria disponibilizado em 15 dias, e que o médico da ESF teria acesso via Conecte SUS.

Novamente o médico, tutor temporário dos dados de Ana, tem acesso aos resultados do exame radiológico, pois, a mesma já havia autorizado o acesso à sua história clínica. Imediatamente, Ana recebe uma notificação no seu celular, com informações do estabelecimento de saúde, profissional, data e hora do acesso, como já mencionado.

Durante visita do Agente Comunitário de Saúde (ACS) à casa de Ana, ela relatou que havia realizado a mamografia há 17 dias e que gostaria de saber se o médico já tinha acesso ao resultado. O ACS se compromete, então, a verificar no sistema a situação para Ana, sem a necessidade de ela ir à UBS.

O ACS entra em contato com os profissionais de saúde cadastrados no Conecte SUS Profissional, que estão acompanhando o caso de Ana, para saber se o laudo do exame radiológico já foi emitido.

Ana fica em casa... e continua com seus afazeres domésticos: o almoço dos filhos, a hora do colégio e os cuidados com a casa.

O médico da ESF acessou, então, o resultado da mamografia de Ana via Conecte SUS, 20 dias após a realização da mesma, analisou o laudo e solicitou ao ACS que avisasse Ana da necessidade do agendamento de uma consulta com ele, que ela mesma faria pelo aplicativo.

[7] Interoperabilidade semântica: Capacidade de troca de informações entre diferentes pontos da Rede de Atenção à Saúde por meio de termos-padrão.

Ana recebe mais uma notificação de acesso aos seus dados, com a identificação do médico que o fez, e uma notificação do agendamento da consulta para o dia seguinte.

No dia seguinte, durante o atendimento, o médico da ESF comunica à Ana a necessidade de realização de uma biópsia, com base no protocolo de casos como o dela, pois, o laudo mamográfico apontou uma neoplasia. Angustiada, Ana questiona se o caso é grave. O médico esclareceu que seria necessário fazer o exame o mais rápido possível, pois, se fosse confirmado o câncer, quanto mais cedo o tratamento fosse iniciado, maior seria a chance de cura. Ele então solicitou a biópsia, conforme as regras do município, via sistema de regulação, cujo agendamento teria uma fila de espera de dois meses.

O tráfego dos dados entre a UBS e o sistema de regulação do agendamento também é mantido sob proteção para que não sejam acessados indevidamente por terceiros.

Ana foi notificada, via Conecte SUS, sobre a data, horário e local em que ela realizaria o exame e que seria feito na Capital. Ao longo dos dois meses em que esperou, fez uso analgésicos prescritos para o controle da dor e enfrentou uma angústia diária.

Após dois meses de espera, Ana vai à Capital para ser submetida à biópsia da mama. A técnica de enfermagem informa que o laudo ficará pronto em dez dias. Dez dias após a realização da biópsia, o médico de Ana recebeu a notificação da liberação do laudo do exame histopatológico da mesma. Ele realizou o agendamento prioritário de Ana para o atendimento especializado com um mastologista, via sistema de regulação. A consulta ficou agendada para a semana seguinte na Capital.

O tráfego de dados entre o laboratório de análises clínicas, o médico da UBS, o sistema de regulação, o mastologista e Ana também ocorre com segurança pela tecnologia blockchain e a verificação do serviço de elegibilidade[8]. Novamente, ela recebe notificações em seu celular sobre a identidade de todos os profissionais da RAS que acessaram seus dados e a finalidade de cada acesso.

[8] Serviço de elegibilidade: é utilizado para definir se o profissional de saúde está habilitado ou não a acessar os dados do cidadão, aplicando regras de vinculação do profissional com o estabelecimento de saúde, CPF, categoria profissional, certificação da instalação de prontuário eletrônico, entre outros.

Já na Capital, no Hospital Estadual, que era credenciado como Cacon, Ana foi recebida pelo mastologista que a examinou e analisou os laudos de seus exames. O mastologista informou à Ana que ela possuía um nódulo maligno, de aproximadamente 1 cm, e que não havia, aparentemente, um comprometimento clínico da sua cadeia linfática axilar. Informou, ainda, que Ana seria submetida a uma cirurgia para a retirada do nódulo com possibilidade de não precisar retirar a mama toda.

Para dar seguimento ao preparo pré-operatório de Ana, o mastologista prescreveu exames para saber exatamente qual era o seu estado geral de saúde e para que ele pudesse tomar as melhores decisões. O mastologista solicitou à Ana, também, ainda que estivesse assintomática, a testagem para a covid-19, considerando todos os riscos aos quais Ana vinha se expondo em suas viagens à Capital.

Cerca de três meses foram necessários para que todos os exames de Ana ficassem prontos. A cirurgia foi planejada e Ana assinou o termo de consentimento informado para realização do procedimento, tendo a ciência de que a sua mama poderia ser retirada.

Esses dados sobre a cirurgia também foram armazenados na nuvem[9], por meio do servidor online, e podem ser acessados pelo mastologista, durante o atendimento e pela própria Ana, a qualquer momento.

O resultado do exame molecular para a covid-19 foi negativo e, tanto o médico, quanto Ana tiveram acesso a esse resultado via Conecte SUS. Isso foi possível devido à integração do Gerenciador de Ambiente Laboratorial (GAL), que interliga os processos de análises laboratoriais à RNDS.

Usando o aplicativo Conecte SUS Cidadão no seu celular, Ana teve acesso aos resultados do exame de covid-19 de forma precisa, com segurança, sem a necessidade de ir até o laboratório buscar o laudo do exame.

Na data marcada, Ana foi internada para ser submetida à cirurgia. Foi retirada parte da mama, mas, não houve prejuízo estético, nem a necessidade de retirar os linfonodos axilares. A cirurgia foi um sucesso e, após quatro dias, Ana recebeu alta hospitalar e foi encaminhada para o tratamento radioterápico, o que é recomendado quando o tratamento cirúrgico é conservador.

[9] Nuvem (Cloud): tecnologia que permite guardar dados na Internet por meio de um servidor online. Por se tratar de dados sensíveis, a RNDS garante que as atividades de tratamento de dados pessoais e sensíveis atenderão aos princípios da LGPD.

O prontuário de Ana, com todo seu histórico clínico, é de sua titularidade, ou seja, os dados são de propriedade da Ana e permanecem acessíveis por ela a qualquer momento. Os profissionais que não estão mais acompanhando o caso de Ana não podem mais acessar seu histórico clínico.

Ana precisou passar por uma consulta de retorno com o oncologista que foi agendada para dali quatro semanas, mas, Ana recebeu mensagem no seu celular sobre o surgimento de uma vaga e a antecipação da sua consulta para a próxima semana.

O oncologista, cadastrado no Conecte SUS Profissional, passou a ter a tutela temporária sobre os dados da Ana, como os outros profissionais que estavam cuidando dela anteriormente.

Devido às características do tumor, Ana precisou fazer uso de hormonioterapia contínua por cinco anos, além da radioterapia já indicada. Não houve a necessidade de tratamento quimioterápico.

Durante o caso de Ana, foram garantidos o sigilo e a confidencialidade dos dados, e somente os profissionais de saúde envolvidos no atendimento dela puderam ter acesso aos seus dados de saúde.

Vamos refletir?

Foi possível observar que, em todo o tráfego de dados de saúde de Ana entre os profissionais durante o contato assistencial, os estabelecimentos que compõem a RAS e a cidadã, houve proteção para garantir segurança e confidencialidade desses dados. Ana, como titular, ou seja, proprietária dos seus dados de saúde, recebeu notificação no aplicativo Conecte SUS Cidadão sempre que sua história clínica foi acessada.

Para relembrar...

- Quem é o proprietário/titular dos dados em saúde? É o cidadão que recebe o atendimento em um estabelecimento de saúde.
- E o profissional de saúde também é proprietário dos dados? Não. Ele é um tutor temporário dos dados e pode acessá-los somente se estiver autorizado e envolvido no atendimento ao cidadão.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM **SAÚDE DIGITAL**

Segurança e ética no compartilhamento de dados pessoais de saúde

Unidade 3

Estratégias para engajamento e conscientização do profissional e do cidadão

Ana Laura de Sene Amâncio Zara,
Rejane Faria Ribeiro-Rotta,
Renata Dutra Braga,
Sheila Mara Pedrosa,
Silvana de Lima Vieira dos Santos,
Suse Barbosa Castilho



Unidade 3: Estratégias para Engajamento e Conscientização do Profissional

3.1 Dicas e Orientações para os Profissionais e Gestores

Elaboramos, a partir da ferramenta Vyond[1], algumas dicas e orientações para você profissional ou gestor da área da saúde:



3.2 Dicas e Orientações para os Cidadãos

Elaboramos, a partir da ferramenta Vyond, algumas dicas e orientações para você Cidadão, usuário do SUS:



3.3 Jogo sério

Vamos praticar um pouco desses conceitos apreendidos até aqui? E faremos isso por meio de um jogo.

A expansão das estratégias de gamificação tem permitido a utilização de jogos não apenas para o entretenimento, mas também no processo de educação, desenvolvimento de habilidades e competências. São várias as classificações e gêneros desses jogos[35].

- **O jogo:** O tipo de jogo que apresentamos aqui é o jogo sério (*serious game*), do gênero *Role-playing game* (RPG), sendo um jogo narrativo, onde não haverá ganhadores ou perdedores, mas uma interação com personagens na busca do fortalecimento do conhecimento sobre a temática desenvolvida neste microcurso.
- **O contexto:** O caso de Ana
- **Objetivo:** O jogador controla a personagem Ana (utilizando setas e barra de espaços do teclado OU mouse) em sua trajetória pelo o sistema de saúde, interagindo com os objetos do ambiente e com diferentes personagens. Nessa trajetória serão demonstrados os benefícios da RNDS e as vantagens da saúde digital no processo de diagnóstico e tratamento do câncer de mama de uma cidadã brasileira
- **Fases:** O jogo tem cinco fases e para a mudança de fase, o jogador deverá encontrar um conjunto de informações que completam as diferentes fases da trajetória da Ana no processo de diagnóstico e tratamento do seu câncer de mama.
  - Fase 1: Encontrar o celular e o CPF de Ana
  - Fase 2: Conseguir cinco respostas para conseguir falar com a enfermeira chefe
  - Fase 3: Encontrar o celular de Ana
  - Fase 4: Ir para consulta com o médico
  - Fase 5: Ir para a cirurgia



EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM **SAÚDE DIGITAL**

Segurança e ética no compartilhamento de dados pessoais de saúde

Unidade 4

Encerramento do microcurso

Ana Laura de Sene Amâncio Zara,
Rejane Faria Ribeiro-Rotta,
Renata Dutra Braga,
Sheila Mara Pedrosa,
Silvana de Lima Vieira dos Santos

Unidade 4: Encerramento do Microcurso 3

Os microcursos do Programa Educacional de Saúde Digital da UFG buscam, dentre seus vários objetivos, fortalecer cada vez mais o papel do profissional de saúde no fornecimento da informação de qualidade e para o engajamento e conscientização do cidadão quanto à autorização do acesso aos seus dados pessoais de saúde e uso dos dados para o seu melhor acompanhamento na Rede de Atenção à Saúde.

Este microcurso, em especial, apresentou-lhes, e por vezes reforçou, os vários aspectos e meios relacionados à ética e segurança dos dados da saúde do cidadão a serem compartilhados. Vocês foram instigados à reflexão sobre o papel dos profissionais envolvidos na atenção à saúde e também a se reconhecerem nesse cenário.

Esperamos que vocês estejam convencidos da importância e da necessidade de mudança de paradigmas sobre o acesso aos dados de saúde do cidadão de maneira segura, pela Rede Nacional de Dados em Saúde.

Assim, ao respeitarmos a vontade do cidadão, resguardando a confidencialidade e a privacidade da sua intimidade, bem como reconhecendo que esse é melhor caminho, faremos com que o Brasil dê um grande passo rumo à melhoria da qualidade da atenção à saúde.

Referências

1. SERPRO. **SERPRO e LGPD: segurança e inovação.** Acesso em 22 jun. 2020. Disponível em: https://www.serpro.gov.br/lgpd/

2. SOARES, P. V. C. **Guia LGPD: Lei Geral de Proteção aos Dados Simplificada.** Acesso em 22 jun. 2020. Disponível em: https://d335luupugsy2.cloudfront.net/cms/files/92859/1565723282Guia_-_LGPD.pdf

3. ASSIS E MENDES ADVOGADOS. **Histórico das leis de proteção de dados e da privacidade na Internet.** Acesso em 22 jun. 2020. Disponível em: https://assisemendes.com.br/blog/historico-protecao-de-dados/

4. BRASIL. **Constituição da República Federativa do Brasil de 1988.** Acesso em 22 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

5. BRASIL. **Lei Nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Acesso em 22 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm

6. BRASIL. **Lei Nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei Nº 8.112, de 11 de dezembro de 1990; revoga a Lei Nº 11.111, de 5 de maio de 2005, e dispositivos da Lei Nº 8.159, de 8 de janeiro de 1991; e dá outras providências.** Acesso em 22 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

7. BRASIL. **Lei Nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Acesso em 22 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

8. BRASIL. **Decreto Nº 7.962, de 15 de março de 2013. Regulamenta a Lei Nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.** Acesso em 22 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm

9. BRASIL. **Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União, Brasília, DF. 2018. Acesso em 8 abr. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

10. BRASIL. MINISTÉRIO DA SAÚDE. **Rede Nacional de Dados em Saúde (RNDS).** Portal do Governo Brasileiro, 2020. Acesso em 22 jun. 2020. Disponível em: https://rnds.saude.gov.br/

11. BRASIL. **Decreto de 29 de novembro de 2017. Dispõe sobre o Conjunto Mí-**

nimo de Dados da Atenção à Saúde. Acesso em 23 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14501.htm

12. BVS. **DeCS - Descritores em Ciências da Saúde.** Acesso em 23 jun. 2020. Disponível em: http://decs.bvs.br/cgi-bin/wxis1660.exe/decsserver/?IsisScript=../cgi-bin/decsserver/decsserver.xis&interface_language=p&previous_page=homepage&previous_task=NULL&task=start

13. BRASIL. MINISTÉRIO DA SAÚDE. **Portaria Nº 639, de 31 de março de 2020. Dispõe sobre a Ação Estratégica "O Brasil Conta Comigo - Profissionais da Saúde", voltada à capacitação e ao cadastramento de profissionais da área de saúde, para o enfrentamento à pandemia do coronavírus (COVID-19).** Acesso em 20 jun. 2020. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-639-de-31-de-marco-de-2020-250847738

14. CONSELHO FEDERAL DE SERVIÇO SOCIAL. **Código de Ética do/a Assistente Social. Lei Nº 8662/93 de Regulamentação da Profissão.** Acesso em 21 jun. 2020. Disponível em: http://www.cfess.org.br/arquivos/CEP_CFESS-SITE.pdf

15. CONSELHO FEDERAL DE BIOLOGIA. **Resolução Nº 2, de 5 de março de 2002. Aprova o Código de Ética do Profissional Biólogo.** Acesso em 20 jun. 2020. Disponível em: https://cfbio.gov.br/2002/03/21/resolucao-no-2-de-5-de-marco-de-2002-2/

16. CONSELHO FEDERAL DE BIOMEDICINA. **Resolução Nº 198, de 21 de fevereiro de 2011. Regulamenta o novo Código de Ética do Profissional Biomédico.** Acesso em 20 jun. 2020. Disponível em: http://cfbm.gov.br/legislacao/codigo-de-etica-da-profissao-de-biomedico/

17. CONSELHO FEDERAL DE EDUCAÇÃO FÍSICA. **Resolução CONFEF Nº 307/2015. Dispõe sobre o Código de Ética dos Profissionais de Educação Física registrados no Sistema CONFEF/CREFs.** Acesso em 20 jun. 2020. Disponível em: https://www.confef.org.br/confef/resolucoes/381

18. CONSELHO FEDERAL DE ENFERMAGEM. **Resolução COFEN Nº 564/2017, de 6 de novembro de 2017. Código de Ética dos Profissionais de Enfermagem.** Acesso em 20 jun. 2020. Disponível em: http://www.cofen.gov.br/wp-content/uploads/2012/03/resolucao_311_anexo.pdf

19. CONSELHO FEDERAL DE FARMÁCIA. **Resolução Nº 596, de 21 de fevereiro de 2014. Dispõe sobre o Código de Ética Farmacêutica, o Código de Processo Ético e estabelece as infrações e as regras de aplicação das sanções disciplinares.** Acesso em 20 jun. 2020. Disponível em: http://www.cff.org.br/userfiles/file/resolucoes/596.pdf

20. CONSELHO FEDERAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL. **Resolução Nº 424, de 8 de julho de 2013.** Acesso em 20 jun. 2020. Disponível em: https://www.coffito.gov.br/nsite/?p=3187

21. CONSELHO FEDERAL DE FONOAUDIOLOGIA. **Código de Ética da Fonoaudiologia.** Acesso em 20 jun. 2020. Disponível em: https://www.fonoaudiologia.org.br/cffa/wp-content/uploads/2016/03/Codigo-de-Etica-2016.pdf

22. CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica. Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM Nº 2.222/2018 e 2.226/2019.** Acesso em 21 jun. 2020. Disponível em: http://portal.cfm.org.br/images/PDF/cem2019.pdf

23. CONSELHO FEDERAL DE MEDICINA VETERINÁRIA. **Resolução Nº 1138, de 16 de dezembro de 2016. Aprova o Código de Ética do Médico Veterinário.** Acesso em 21 jun. 2020. Disponível em: http://portal.cfmv.gov.br/uploads/reso%201138_2016%20portal%20cfmv%20(3).pdf

24. CONSELHO FEDERAL DE NUTRICIONISTAS. **Código de Ética e de Conduta do Nutricionista.** Acesso em 21 jun. 2020. Disponível em: https://www.cfn.org.br/wp-content/uploads/2018/04/codigo-de-etica.pdf

25. CONSELHO FEDERAL DE ODONTOLOGIA. **Código de Ética Odontológica. Resolução CFO-118/2012.** Acesso em 23 jun. 2020. Disponível em: http://website.cfo.org.br/codigos/

26. CONSELHO FEDERAL DE PSICOLOGIA. **Código de Ética Profissional do Psicólogo. Resolução CFP Nº 010/05.** Acesso em 21 jun. 2020. Disponível em: https://site.cfp.org.br/wp-content/uploads/2012/07/codigo-de-etica-psicologia.pdf

27. CONSELHO NACIONAL DE TÉCNICOS EM RADIOLOGIA. **Resolução CONTER Nº 15, de 12 de dezembro de 2011. Dispõe sobre a Reformulação do Código de Ética dos Profissionais das Técnicas Radiológicas. Revoga a Resolução CONTER Nº 6, de 31.05.2006 e seu anexo.** Acesso em 23 jun. 2020. Disponível em: http://www.conter.gov.br/uploads/legislativo/codigodeetica.pdf

28. BRASIL. **Medida Provisória Nº 959, de 29 de abril de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória Nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei Nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.** Acesso em 23 jun. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm

29. MINISTÉRIO DA SAÚDE. SECRETARIA EXECUTIVA. DATASUS. COORDENAÇÃO-GERAL DE INOVAÇÃO EM SISTEMAS DIGITAIS. **Ações para adequação da RNDS à Lei Geral de Proteção de Dados Pessoais.** Acesso em 15 jun. 2020. Disponível em: https://rnds.saude.gov.br/wp-content/uploads/2020/06/Ações-para-a-Adequação-da-RNDS-à-LGPD---24.11.2020.pdf

30. RASIL. **Acesso GOV.BR.** Acesso em 1 jun. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/transformacao-digital/ferramentas/acesso-gov-br

31. BRASIL. MINISTÉRIO DA SAÚDE. **Conecte SUS: Plataforma de saúde para o cidadão, profissionais e gestores de saúde.** Acesso em 1 jun. 2020. Disponível em: https://conectesus.saude.gov.br/home.

32. BRASIL. **Decreto Nº 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.** Acesso em 20 jun. 2020. Disponível em: http://

www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm

33. BRASIL. **Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD).** Acesso em 18 jun. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd

34. BAPTISTA, T. W. F.; MACHADO, C. V.; LIMA, L. D. **O caso de Ana. Qualificação de Gestores do SUS.** Fundação Oswaldo Cruz. Escola Nacional de Saúde Pública. p. 75-91. Acesso em 20 maio 2020. Disponível em: http://www6.ensp.fiocruz.br/repositorio/sites/default/files/arquivos/CasoAna.pdf

35. KAPP, K. M. **The gamification of learning and instruction: game-based methods and strategies for training and education**. John Wiley & Sons, 2012.

Minibiografias

Organizadores

Ana Laura de Sene Amâncio Zara é graduada em Farmácia e em Análises Clínicas (UFMT), especialista em Avaliação de Tecnologias em Saúde (UFRGS) e em Docência do Ensino Superior (UCDB). Possui mestrado e doutorado em Epidemiologia pelo Programa de Pós-Graduação em Medicina Tropical e Saúde Pública (UFG) e pós-doutorado pelo Programa de Pós-graduação de Odontologia da Faculdade de Odontologia (UFG). Atualmente, é professora do Departamento de Saúde Coletiva da UFG. Ensina, pesquisa e orienta nas áreas de Epidemiologia, Saúde Coletiva, Metodologia e Editoração Científicas, Economia da Saúde, Bioestatística, Informática em Saúde e Revisões Sistemáticas.

E-mail: analauraufg@gmail.com

Fábio Nogueira de Lucena é graduado em Ciência da Computação (UFG), mestre e doutor em Ciência da Computação (UNICAMP), especialista em Informática em Saúde (UNIFESP), Project Management Professional (PMI) e Certified Software Development Professional (IEEE), além de possuir outras certificações da indústria de software. É professor titular do curso de Engenharia de Software do Instituto de Informática da UFG.

Github: https://github.com/kyriosdata

E-mail: kyriosdata@ufg.br

Rejane Faria Ribeiro-Rotta é graduada em Odontologia (UFG), especialista em Radiologia Bucomaxilofacial e Estomatologia, mestre e doutora em Odontologia (Diagnóstico Bucal) (USP-Bauru), com experiência em colaborações internacionais em pesquisa e intercâmbios, e na gestão institucional do ensino superior. Professora titular da Faculdade de Odontologia da UFG. Fundadora do Centro Goiano de Doenças da Boca da Faculdade de Odontologia da UFG (CGDB-FO-UFG) e da Comissão de Governança da Informação em Saúde da UFG. Principais temáticas de pesquisa: Diagnóstico de lesões da região bucomaxilofacial / Câncer de boca; Dores crônicas orofaciais; Diagnóstico por imagem da região bucomaxilofacial; Prática baseada em evidência, Informação e Informática em saúde.

E-mail: rejanefrr@ufg.br

Renata Dutra Braga é professora adjunta do Instituto de Informática da Universidade Federal de Goiás (UFG). É mestre e doutora em Ciências da Saúde pela Faculdade de Medicina da UFG, pós-graduada em Informática em Saúde (UNIFESP) e em Qualidade e Gestão de Software (PUC-GO) e é graduada em Sistemas de Informação (UniEvangélica). É atualmente vice-coordenadora da Comissão de Governança da Informação em Saúde (CGIS-UFG). Ensina, pesquisa, orienta e desenvolve projetos de extensão na área de saúde digital, com interesse, principalmente em modelagem de processo de negócios, engenharia de requisitos, modelos de informação, terminologias clínicas e padrões para a troca da informação em saúde.

E-mail: renatadbraga@ufg.br

Rita Goreti Amaral é professora titular da Faculdade de Farmácia da Universidade Federal de Goiás (UFG), com atuação na graduação e pós-graduação. Graduada em Farmácia e Bioquímica e especialista em Citologia Clínica (UFG). Mestre em Biologia Celular e Molecular (USP) e Doutora em tocoginecologia pela Faculdade de Ciências Médicas (UNICAMP). Coordenadora do Laboratório de Monitoramento Externa da Qualidade da Faculdade de Farmácia (UFG). Desenvolve projetos de pesquisa e extensão na área de Citologia Clínica e Saúde Pública, atuando nos seguintes temas: controle da qualidade em citopatologia do colo do útero, prevenção, detecção precoce de doenças, aperfeiçoamento de métodos diagnósticos, desenvolvimento e validação de práticas de cuidado do paciente nas doenças crônicas transmissíveis e não transmissíveis, informática em saúde e assistência farmacêutica.

E-mail: rita@ufg.br

Sheila Mara Pedrosa é graduada e mestre em Enfermagem pela Faculdade de Enfermagem (UFG), especialista em Saúde Coletiva e Regulação em Saúde no SUS (IEP/HSL) e doutora em Ciências da Saúde pela Faculdade de Medicina (UFG). Atualmente é professora adjunta do Centro Universitário de Anápolis e desenvolve pesquisa e extensão no âmbito das violências e vulnerabilidade social. É membro da Comissão de Governança da Informação em Saúde (CGIS-UFG) e participa de projetos voltados à saúde digital.

E-mail: sheilaenf@gmail.com

Silvana de Lima Vieira dos Santos - é enfermeira, mestre e doutora em Ciências da Saúde (UFG), Especialista em Enfermagem em Infectologia (USP) e em Informática em Saúde (UNIFESP). É professora associada da Faculdade de Enfermagem (UFG). Vice líder do Núcleo de Estudos e Pesquisa de Enfermagem em Prevenção e Controle de Infecção Relacionada à Assistência à Saúde (NEPIH), vinculado ao CNPq. Experiência na área de prevenção e controle de infecções relacionadas à assistência à saúde, epidemiologia e informática em saúde. Coordenadora da Comissão de Governança da Informação em Saúde (CGIS-UFG).

E-mail: silvanalvsantos@ufg.br

Taciana Novo Kudo é professora adjunta do Instituto de Informática da Universidade Federal de Goiás (UFG). É mestre e doutora em Ciência da Computação pelo Departamento de Computação (UFSCar) e graduada em Ciência da Computação (UNIMAR). Possui experiência profissional na área de Engenharia de Software, especificamente em Engenharia de Requisitos e Gerência de Projetos, em institutos de pesquisa e empresas de São Paulo e Goiás. Como pesquisadora, atua em projetos voltados para Engenharia de Software, Engenharia de Requisitos e Informática aplicada à Educação e à Saúde.

E-mail: taciana@ufg.br

PROGRAMA EDUCACIONAL EM SAÚDE DIGITAL DA UNIVERSIDADE FEDERAL DE GOIÁS

CGIS UFG Comissão de Governança da Informação em Saúde

CIGETS CENTRO DE INOVAÇÃO EM GESTÃO DA EDUCAÇÃO E DO TRABALHO EM SAÚDE

DATASUS DEPARTAMENTO DE INFORMÁTICA DO SUS

Ministério da Saúde

SOBRE O E-BOOK

Tipografia: Montserrat

Publicação: Cegraf UFG
Câmpus Samambaia, Goiânia - Goiás. Brasil. CEP 74690-900
Fone: (62) 3521-1358
https://cegraf.ufg.br