Segurança da informação: realidades na atenção primária em uma metrópole brasileira

Information security: realities in primary care in a Brazilian metropolis

Seguridad de la información: realidades en la atención primaria en una metrópoli brasileña

Rodrigo Cândido Borges[1,2], Silvana de Lima Vieira dos Santos[3], Fábio Nogueira de Lucena[4], Maria Márcia Bachion[3]

1. Programa de Pós-graduação em Ciências da Saúde, Faculdade de Medicina, Universidade Federal de Goiás, Goiânia (GO), Brasil.
2. Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Inhumas (GO), Brasil.
3. Faculdade de Enfermagem, Universidade Federal de Goiás, Goiânia (GO), Brasil.
4. Instituto de Informática, Universidade Federal de Goiás, Goiânia (GO), Brasil.

Autor correspondente: Rodrigo Cândido Borges
E-mail: rodrigo.borges@ifg.edu.br

Resumo

Objetivo: Descrever elementos relativos à segurança da informação no contexto das unidades municipais de atenção primária à saúde de uma metrópole brasileira. **Métodos**: Estudo descritivo-exploratório, transversal, realizado entre maio/2019 e fevereiro/2020, na cidade de Goiânia, estado de Goiás. A população do estudo foi constituída de profissionais que atuam nos Centros de Saúde e Centros de Saúde da Família. **Resultados**: Entre as 72 unidades de saúde avaliadas, em aproximadamente 95% destas não há controle de trânsito de pessoas ou identificação de profissionais, usuários, acompanhantes, visitantes ou prestadores de serviços. Cerca de 91% dos profissionais revelaram nunca ter participado de treinamentos sobre segurança da informação e 36,5% citaram ter compartilhado suas credenciais exclusivas de acesso aos sistemas de informação em saúde com terceiros. **Conclusão**: Não há política de segurança de informação estabelecida. A pesquisa contribuiu para a geração de

conhecimentos que podem alicerçar futuros processos de tomada de decisões pelos gestores de saúde.

Descritores: Atenção primária à saúde; Saúde digital; Segurança da informação; Tecnologia em saúde.

Abstract

Objective: To describe elements related to information security in the context of municipal primary health care units in a Brazilian metropolis. **Methods:** Descriptive-exploratory study, cross-sectional, carried out between May/2019 and February/2020, in the city of Goiânia, state of Goiás. The study population consisted of professionals who work in Health Centers and Family Health Centers. **Results:** Among the 72 health units evaluated, in approximately 95% of these there is no control over the transit of people or identification of professionals, users, companions, visitors or service providers. About 91% of professionals revealed that they had never participated in information security training and 36.5% mentioned having shared their unique credentials to access health information systems with third parties. **Conclusion:** There is no established information security policy. The research contributed to the generation of knowledge that can underpin future decision-making processes by health managers.

Descriptors: Primary health care; Digital health; Information security; Health technology.

Resumen

Objetivo: Describir los elementos relacionados con la seguridad de la información en el contexto de las unidades de atención primaria de salud municipales en una metrópoli brasileña. **Métodos:** Estudio descriptivo-exploratorio, transversal, realizado entre mayo/2019 y febrero/2020, en la ciudad de Goiânia, estado de Goiás. La población de estudio estuvo constituida por profesionales que actúan en Centros de Salud y Centros de Salud de la Familia. **Resultados:** Entre las 72 unidades de salud evaluadas, en aproximadamente el 95% de estas no existe control sobre el tránsito de personas o identificación de profesionales, usuarios, acompañantes, visitantes o prestadores de servicios. Cerca del 91% de los profesionales reveló que nunca había participado en

capacitación en seguridad de la información y el 36,5% mencionó haber compartido sus credenciales únicas para acceder a los sistemas de información en salud con terceros. **Conclusión:** No existe una política de seguridad de la información establecida. La investigación contribuyó a la generación de conocimiento que pueda sustentar futuros procesos de toma de decisiones por parte de los gestores de salud.
Descriptores: Atención primaria de salud; Salud digital; Seguridad de la información; Tecnología de la salud.

Introdução

O Brasil é um país de dimensões continentais, com profundas assimetrias regionais, e apesar dos esforços para estruturação e implementação da saúde digital no país, ainda há desafios que comprometem o alcance de um ecossistema de saúde conectada, cabendo ressaltar: a indisponibilidade de computadores modernos, dispositivos móveis e conectividade em parte dos estabelecimentos assistenciais de saúde[1,2]; a não interoperabilidade entre sistemas de informação em saúde[3]; a carência de medidas de segurança para proteção de dados[4]; e a falta de treinamento dos profissionais para uso de TIC[5].

Com a promulgação da Lei Geral de Proteção de Dados Pessoais[6], a segurança dos dados pessoais de saúde passou a ser um direito de todo cidadão. Por consequência, a promoção e manutenção da privacidade e confidencialidade das informações se tornam questões primordiais para o cenário de saúde digital[7].

Para operar de forma confiável, os dispositivos responsáveis pelo processamento, armazenamento e transmissão das informações exigem um ambiente físico apropriado[7]. O acesso ao perímetro onde se encontram tais equipamentos deve ser devidamente controlado, evitando o trânsito de pessoas não autorizadas. Além disso, questões relacionadas à climatização dos ambientes, confiabilidade da rede de energia elétrica e proteção contra chuvas, ventos e incêndios devem ser observadas[8].

Antes da disponibilização de qualquer dado identificado, é essencial que políticas e serviços de segurança sejam estabelecidos e aprimorados[1,5,6]. Informações apresentadas de modo inconsistente podem iniciar uma sequência de ações graves,

colocando em risco a vida de pacientes e interferindo diretamente em decisões que envolvam a gestão, prestação e continuidade do cuidado em saúde[9].

O emprego de controles organizacionais para acesso a dados críticos, autenticação de usuários e proteção contra códigos maliciosos e ataques virtuais favorece para que os dados gerados e armazenados pelos profissionais sejam fidedignos, livres de interceptações que possam alterar informações sensíveis e de cunho privativo[8,10].

Enfim, para que um plano de saúde digital seja implementado, é fundamental que mecanismos de segurança da informação sejam implementados em todos os campos da saúde, o que torna relevante o emprego de ferramentas que possam acompanhar o estágio de adoção destas tecnologias[5].

Com o propósito de explorar esta conjuntura e contribuir para avaliá-la melhor, este estudo tem como finalidade descrever elementos associados à segurança da informação nas unidades municipais de atenção primária à saúde de uma grande cidade brasileira, revelando elementos presentes nestes cenários e apresentando fatores que possam ser levados em conta na elaboração de futuras políticas.

Métodos

Estudo descritivo-exploratório, do tipo transversal, realizado no período de maio de 2019 a fevereiro de 2020 na cidade de Goiânia-GO, metrópole com uma população de aproximadamente 1,5 milhão de habitantes localizada na Região Centro-Oeste do Brasil, e cuja rede municipal de atenção à saúde é constituída de: 59 Centros de Saúde da Família (CSF), 22 Centros de Saúde (CS), 21 Unidades de Atendimento à Saúde Mental, 9 Centros de Atenção Integrada à Saúde (CAIS), 4 Centros Integrados de Atenção Médico Sanitária (CIAMS), 2 Unidades de Pronto Atendimento (UPA), 2 Hospitais Maternidades, 1 Ambulatório de Queimaduras, 1 Centro de Referência em Ortopedia e Fisioterapia e 1 Centro de Referência em Diagnóstico e Terapêutica[11].

Para a presente pesquisa, realizada com recorte da atenção primária à saúde, foram avaliados 50 CSF e todos os CS. Por conta do início da pandemia de COVID-19, 9 CSF não foram abordados, configurando em perdas.

Os quadros profissionais destas unidades englobam enfermeiros, odontólogos, médicos, farmacêuticos, entre outros; além de técnicos em saúde, auxiliares em saúde, agentes administrativos, agentes de apoio administrativo e assistentes administrativos. Os CSF ainda contam com os agentes comunitários de saúde, profissionais que realizam a integração dos serviços de saúde da atenção primária com a comunidade por meio de visitas domiciliares.

A população do estudo foi constituída de profissionais que atuavam nos estabelecimentos de saúde citados. A amostra randomizada foi composta por 50% de servidores que satisfaziam aos seguintes critérios de inclusão: utilizar sistemas de informação em saúde no processo de trabalho nas respectivas unidades e estar atuando nos estabelecimentos de saúde, no período estipulado para a coleta de dados. Foram consideradas perdas os casos de servidores que operavam sistemas de informação em saúde e encontravam-se em período de férias ou licença na data estipulada para coleta de dados. Durante o período de coleta de dados esse contingente representou fração ≤ 5%.

Com base na lista dos servidores em atividade no período de realização do estudo, efetuou-se a estratificação dos profissionais segundo as áreas de atuação (enfermeiros, odontólogos, médicos, outros profissionais especialistas em saúde, técnicos em saúde, auxiliares em saúde e servidores administrativos) e aplicou-se processo de seleção aleatória de 50% dos servidores de cada área por meio do software *Random Number Generator*[12].

No processo de recrutamento dos profissionais, foi apresentada a cada um a natureza do estudo, seus objetivos e procedimentos previstos. Ao verificar o interesse na participação, foi apresentado o Termo de Conhecimento Livre e Esclarecido e combinou-se o momento de coleta de dados.

O recrutamento ocorreu no local de trabalho e aqueles que aceitaram participar assinaram o Termo de Conhecimento Livre e Esclarecido.

Para a coleta de dados utilizou-se questionário elaborado com base na revisão da literatura[1,2,7] contendo trinta e seis questões fechadas, organizadas em eixos que abordavam a caracterização demográfica, socioeconômica e profissiográfica, habilidades no uso recursos de informática, sistemas de informação utilizados no

processo de trabalho na atenção primária à saúde e tópicos associados à segurança da informação.

Cada participante recebeu uma via impressa do questionário e foi acompanhado durante o preenchimento, que demandou em média 20 minutos. Adicionalmente foi realizada observação em campo, mediante roteiro, para verificar os recursos de informática disponíveis.

Para apreciação e sumarização do conjunto de informações obtidas foi realizada análise estatística descritiva. Ainda, a análise também foi direcionada pelas recomendações e perspectivas traçadas pela Política Nacional de Informação e Informática em Saúde[10], estratégias de Saúde Digital para o Brasil[1,5], Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil e Norma ABNT NBR ISO 27799:2019[7].

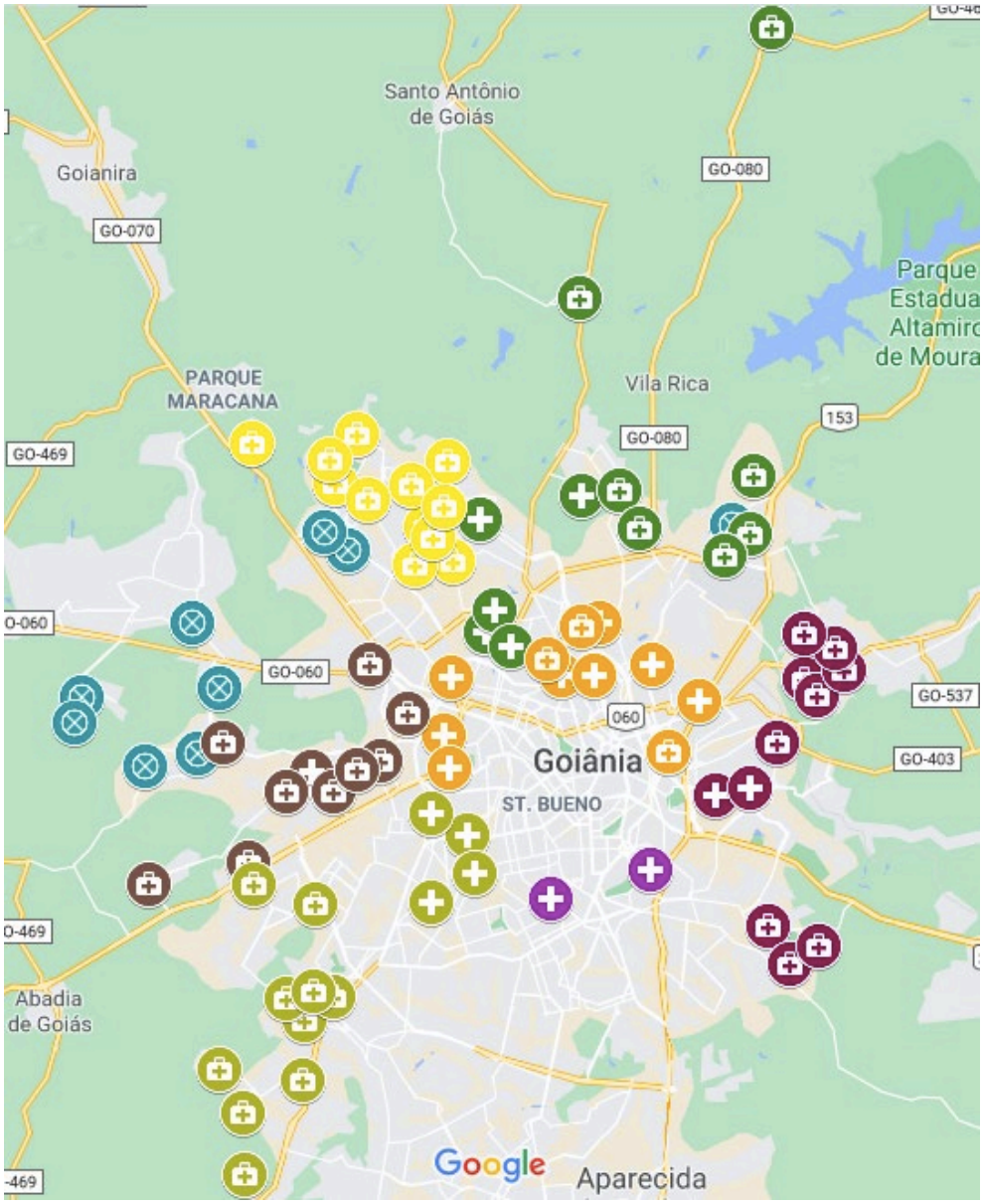
Esta pesquisa integra o projeto "Nível de Maturidade da Infraestrutura de Tecnologia da Informação e Comunicação em Unidades Municipais de Saúde de uma Metrópole Brasileira", autorizado pela Secretaria Municipal de Saúde de Goiânia e aprovado pelo Comitê de Ética e Pesquisa do Hospital das Clínicas da UFG (CAAE 10224919.7.0000.5078 - Parecer nº 3.388.680).

O estudo respeita princípios éticos de pesquisas envolvendo seres humanos definidos em diretrizes nacionais e internacionais[13]. Os participantes deste estudo têm assegurado anonimato e o caráter voluntário.

Resultados e Discussão

Na cidade de Goiânia, as unidades municipais de atenção primária à saúde são distribuídas entre 7 distritos sanitários: Campinas-Centro, Leste, Oeste, Norte, Noroeste, Sul e Sudoeste (Figura 1).

Figura 1 - Estabelecimentos municipais de atenção primária à saúde avaliados divididos por regiões, Goiânia, JUL 2019 - MAR 2020



- Distrito Campinas Centro - Centros de Saúde
- Distrito Campinas Centro - Centros de Saúde da Família
- Distrito Norte - Centros de Saúde
- Distrito Norte - Centros de Saúde da Família
- Distrito Noroeste - Centros de Saúde da Família
- Distrito Oeste - Centros de Saúde
- Distrito Oeste - Centros de Saúde da Família
- Distrito Sul - Centros de Saúde
- Distrito Sudoeste - Centros de Saúde
- Distrito Sudoeste - Centros de Saúde da Família
- Distrito Leste - Centros de Saúde
- Distrito Leste - Centros de Saúde da Família
- Centros de Saúde da Família não avaliados

Fonte: Elaborado pelos autores.

Geograficamente, cada distrito sanitário está ligado a uma região da metrópole (Figura 1), sendo responsáveis pela supervisão técnica e administrativa das ações de vigilância e atenção à saúde da população residente em sua área de abrangência.

Nos CSF e CS avaliados, havia no período de coleta de dados um contingente de 2.047 trabalhadores em atividade. Para participar do estudo foram convidados 1.089 profissionais, 63 recusaram.

Logo, a pesquisa envolveu 1.026 profissionais que utilizavam sistemas de informação em saúde no desenvolvimento de suas atividades, sendo: 761 participantes vinculados aos Centros de Saúde da Família, e 265 aos Centros de Saúde.

O perfil demográfico daqueles que participaram do estudo revelou uma predominância de profissionais do sexo feminino (86,7%) e autodeclarados pardos (58,4%).

Prevalecem nos CSF os agentes comunitários de saúde (ensino fundamental completo) e especialistas em saúde (ensino superior completo), com jornada de 31 a 40 horas, enquanto nos CS preponderam os técnicos em saúde (curso profissionalizante completo) e especialistas em saúde (ensino superior completo), com jornada de 21 a 30 horas. Os profissionais que atuam na administração totalizaram 20,4% nos CSF e 37,4% nos CS.

Para que as estratégias de segurança da informação sejam efetivamente implementadas, é essencial que as organizações de saúde estabeleçam uma política de segurança da informação[7,14]. Um documento, contendo normas e recomendações a serem seguidas pelos estabelecimentos assistenciais de saúde, deve ser aprovado pelo órgão de administração, publicado e comunicado a todos os colaboradores e partes externas relevantes[7].

Apesar disso, nas investigações realizadas *in loco* nos Centros de Saúde e Centros de Saúde da Família constatou-se a ausência de uma política de segurança da informação em todos os estabelecimentos.

Quanto às medidas para segurança física dos equipamentos de informática, constatou-se que o perímetro das áreas com computadores é protegido por paredes, telhados e portas em todos os estabelecimentos, apesar do acesso a estas áreas, predominantemente, não ser controlado. Nenhum dos Centros de Saúde e Centros de

Saúde da família dispõe de sistemas para fornecimento ininterrupto de energia. Para proteção contra incêndios, os extintores de pó químico (tipos BC e ABC) são as soluções mais aplicadas, estando disponíveis em cerca de 97% das unidades investigadas.

A implementação de medidas de segurança física nos perímetros dos estabelecimentos assistenciais de saúde é especialmente desafiadora, afinal, as configurações destes contribuem para que o público tenha um amplo acesso aos espaços operacionais[7]. Todavia, *"independentemente do tamanho, localização e modelo de prestação de serviços, todas as organizações de saúde precisam ter controles rigorosos instalados para proteger a informação de saúde a eles confiada"*[7].

Em relação aos serviços de segurança patrimonial, mais de 40% dos estabelecimentos não possuem qualquer serviço implementado, enquanto 55,6% das unidades de saúde contam com sistema de alarme monitorado.

Quanto à implementação de sistemas de identificação, nenhuma das unidades de saúde avaliadas contam com posto para controle de acesso. Em 94,4% dos estabelecimentos visitados, os profissionais não fazem o uso de crachás ou cartões de identificação. Indivíduos que não fazem parte da força de trabalho da unidade de saúde não são identificados por meio de crachás ou cartões, como visitante, usuário ou prestador de serviço em qualquer das unidades apreciadas.

O emprego de mecanismos de vigilância patrimonial e segurança eletrônica favorece o monitoramento dos ambientes, contribuindo para preservar a segurança física dos trabalhadores da saúde e sujeitos do cuidado, e evitar ações que envolvam o roubo de dados e equipamentos[15].

Nenhuma das unidades de saúde avaliadas estabelecem diretrizes para a classificação das informações, assim, regras sobre o manuseio de dados de acordo com seus níveis de confidencialidade não são definidas.

Sobre a segurança das redes locais sem fio, em todas as unidades municipais de atenção primária à saúde foi detectada a adoção de protocolos de segurança para proteção das trocas de dados nestas redes. A encriptação promovida pelo protocolo *Wi-Fi Protected Access* (WPA, WPA2 e WPA3), contribui para que intrusos não

interceptem as comunicações a fim de violar as mensagens propagadas por radiofrequência[15].

Segundo 88,1% dos participantes, o acesso a todos os sistemas de informação em saúde por eles utilizados é feito via credencial individual. Contudo, dentre o grupo de participantes que fazem uso de senhas para acesso a estes sistemas, 36,5% já compartilharam suas credenciais exclusivas com outras pessoas que atuam no serviço.

Ainda, cerca de 92% dos profissionais compartilham o uso dos computadores disponibilizados pelos estabelecimentos com outros colegas, ao passo que 20,6% e 4,6% destes, respectivamente, relataram ter usado estas máquinas para acesso a e-mail pessoal e rede social.

O comportamento dos sujeitos é reconhecido como um ponto chave para que as práticas de gestão de segurança da informação sejam efetivas[7,16]. O ato de compartilhar credenciais exclusivas de acesso aos sistemas de informação em saúde pode resultar em graves consequências, podendo os envolvidos, inclusive, responder civil e criminalmente pelos transtornos decorrentes de suas condutas[4,16]. A exposição de dados pessoais ou o seu uso de maneira imprópria, pode abrir espaços para tratamentos discriminatórios e fraudes, colocando em risco a saúde física e mental de seus titulares[17].

No que se refere à integridade e confiabilidade das informações registradas por meios dos sistemas de informação em saúde utilizados (Tabela 1), 26% dos participantes não consideram as informações armazenadas íntegras e confiáveis.

Tabela 1 - Opiniões dos profissionais em relação à integridade e confiabilidade das informações registradas por meio dos sistemas de informação em saúde, Goiânia, JUL 2019 - MAR 2020

Apontamentos	**CSF*** ***f* (%)**	**CS**** ***f* (%)**	***f***	**%**
São confiáveis e íntegras	166 (21,8)	63 (23,8)	229	22,3
São parcialmente confiáveis e íntegras	261 (34,3)	87 (32,9)	348	34,0
Não são confiáveis e íntegras	216 (28,4)	52 (19,6)	268	26,0
Não sabem	100 (13,1)	52 (19,6)	152	14,8
Não responderam	18 (2,4)	11 (4,1)	29	2,9

*Centros de Saúde da Família e **Centros de Saúde.
Fonte: Elaborado pelos autores.

Quanto ao preparo dos profissionais acerca da segurança da informação (Tabela 2), mais de 91% dos participantes nunca participou de treinamentos relacionados à temática.

Tabela 2 - Participação dos profissionais dos Centros de Saúde da Família (n=761) e Centros de Saúde (n=265) em treinamentos sobre segurança da informação, Goiânia, JUL 2019 - MAR 2020

Realizaram treinamentos sobre segurança da informação	**CSF*** ***f* (%)**	**CS**** ***f* (%)**	***f***	**%**
Sim	48 (6,3)	16 (6,0)	64	6,3
Não	697 (91,6)	239 (90,2)	936	91,1
Não responderam sobre o assunto	16 (2,1)	10 (3,8)	26	2,6

*Centros de Saúde da Família e **Centros de Saúde.
Fonte: Elaborado pelos autores.

Para que as ações de saúde digital se desenvolvam, é essencial que os trabalhadores da saúde se capacitem e tenham ciência de seus deveres enquanto guardiões de informações pessoais[7,10].

De acordo com a Estratégia e-Saúde para o Brasil:

> A promoção e manutenção da privacidade e confidencialidade das informações identificadas em saúde é uma questão basilar [...], pois quebras de segurança podem causar danos reais a pacientes. Políticas e serviços de segurança e privacidade devem ser implementados antes que qualquer dado identificado seja disponibilizado em um ambiente compartilhado, e devem ser aprimorados conforme se diversifiquem os canais de acesso e os usuários[1].

Em um cenário onde inexistem políticas dirigidas à proteção das informações, medidas para classificação de dados não são estabelecidas, e grande parte dos profissionais não participaram de formações envolvendo informática em saúde, o planejamento, a implantação e o fortalecimento de mecanismos de segurança física e lógica se tornam emergenciais[4,7,16].

Conclusão

A descrição das conjunções de segurança da informação revela um cenário crítico e desafiador, principalmente diante do estabelecido pela Lei Geral de Proteção de Dados Pessoais e Política Nacional de Informação e Informática em Saúde. A quase inexistência de medidas de segurança deve dar lugar à implementação de controles físicos, organizacionais e tecnológicos, com o engajamento dos múltiplos atores da saúde.

Logo, a aproximação entre o poder público e instituições de saúde, de fomento, e de lideranças e especialistas das esferas municipal, estadual e federal torna-se fundamental para que planos de ações sejam construídos de forma coletiva, alicerçando tomada de decisões em favor de um ecossistema de saúde conectada e segura.

Referências

1. Ministério da Saúde (BR), Comitê Gestor da Estratégia de e-Saúde. Estratégia e-Saúde para o Brasil. Brasília, DF; 2017.

2. Núcleo de Informação e Coordenação do Ponto BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2019. São Paulo: Comitê Gestor da Internet no Brasil; 2020.

3. Lucena FN, Ribeiro-Rotta RF, Braga RD. Estrada goiana da informação em saúde: uma concepção. Goiânia: Editora UFG; 2019.

4. Aragão SM, Schiocchet T. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. Revista Eletrônica de Comunicação, Informação e Inovação em Saúde. 2020;14(3).

5. Ministério da Saúde (BR), Secrataria-Executiva, Departamento de Informática do SUS. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília, DF; 2020.

6. Presidência da República (BR), Secretaria-Geral, Subchefia para Assuntos Jurídicos. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF; 2018.

7. Associação Brasileira de Normas Técnicas. ABNT NBR ISO 27799 - Gestão de segurança da informação em saúde utilizando a ISO/IEC 27002. Rio de Janeiro: ABNT; 2019.

8. Hintzbergen K, BAARS H, Hintzbergen J, Smulders A. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport; 2018.

9. Caldeira C, Sarlet GBS. O consentimento informado e a proteção de dados pessoais de saúde na internet. Civilistica.com. 2019;8(1):2-27.

10. Ministério da Saúde (BR). Portaria nº 1.768, de 30 de julho de 2021. Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a PNIIS. Diário Oficial da União. 2 ago 2021; Seção 1:45.

11. Prefeitura de Goiânia, Secretaria Municipal de Saúde. Relação das unidades de saúde da SMS Goiânia [Internet]. Goiânia: SMS Goiânia; 2022 [citado 28 out 2022]. Disponível em: https://www.saude.goiania.go.gov.br.

12. Chiou A. Random Number Generator Plus - Dice, Lotto, Coins [Internet]. Fremont: Random Apps Inc; 2022 [citado 28 out 2022]. Disponível em: https://play.google.com.

13. Council for International Organizations of Medical Sciences. CIOMS. Geneva: CIOMS; 2022 [citado 28 out 2022]. Disponível em: https://cioms.ch.

14. Keshta I, Odeh A. Security and privacy of electronic health records: concerns and challenges. Egyptian Informatics Journal. 2021; 22(2): 177-183.

15. Marcondes JS. Segurança Física. São Paulo: IBRASEP; 2020 [citado 28 out 2022]. Disponível em: https://gestaodesegurancaprivada.com.br.

16. Bredariol Junior JB, et al. Grau de maturidade da segurança da informação na visão dos gestores da rede pública de hospitais federais do Brasil. Revista Ibérica de Sistemas e Tecnologias de Informação, 2021;E41: 232-243.

17. Alves JC. Breves considerações à Lei Geral de Proteção de Dados (LGPD) e sua consonância com o direito fundamental à saúde em tempos de pandemia do novo coronavírus. Revista de Direito e Atualidades. 2021;1(1).