COMMENTARY

Relevance of cybersecurity in maintaining the integrity of reproductive healthcare services

DOI: 10.29063/ajrh2025/v29i12s.2

Suliman MM. Abakar[1], Abdalilah Alhalangy[2] and Saleh A. Alkhamis[3]*

Department of Cybersecurity, College of Computer, Qassim University, Buraydah, Saudi Arabia[1]; Department of Computer Engineering, College of Computer, Qassim University, Buraydah, Saudi Arabia[2]; Department of Cybersecurity, College of Computer, Qassim University, Saudi Arabia[3]

***For Correspondence:** Email: *s.abakar@qu.edu.sa*

Abstract

The digitalization of reproductive healthcare—from teleconsultations to electronic medical records and mobile fertility applications—has improved access, efficiency, and continuity of care. However, this transformation has simultaneously introduced significant cybersecurity vulnerabilities that directly threaten the confidentiality, integrity, and reliability of reproductive health services. Because reproductive health information is deeply sensitive, breaches can lead to severe social, psychological, and clinical consequences. This commentary discusses the growing relevance of cybersecurity in reproductive healthcare delivery, outlines key vulnerabilities across digital care pathways, and emphasizes the ethical and governance imperatives for safeguarding reproductive health data. The paper argues that cybersecurity is not merely a technical requirement but an essential component of reproductive healthcare quality and patient protection. *(Afr J Reprod Health 2025; 29 [12s]: 14-17).*

Keywords: Health Administration; Mobile Health; Telemedicine; Cybersecurity in Healthcare; Cybersecurity in Reproductive Telehealth

Résumé

La numérisation des soins de santé génésique – des téléconsultations aux dossiers médicaux électroniques en passant par les applications de fertilité mobiles – a amélioré l'accès, l'efficacité et la continuité des soins. Cependant, cette transformation a simultanément introduit des vulnérabilités significatives en matière de cybersécurité qui menacent directement la confidentialité, l'intégrité et la fiabilité des services de santé génésique. Étant donné que les informations sur la santé génésique sont profondément sensibles, les violations peuvent entraîner de graves conséquences sociales, psychologiques et cliniques. Ce commentaire examine la pertinence croissante de la cybersécurité dans la prestation des soins de santé génésique, décrit les vulnérabilités clés le long des parcours de soins numériques, et souligne les impératifs éthiques et de gouvernance pour la protection des données de santé génésique. L'article soutient que la cybersécurité n'est pas seulement une exigence technique, mais une composante essentielle de la qualité des soins de santé génésique et de la protection des patientes. *(Afr J Reprod Health 2024; 29 [12s]: 14-17).*

Mots-clés: Administration de la santé, Santé mobile, Télémédecine, Cybersécurité dans les soins de santé, Cybersécurité dans la télésanté reproductive

Introduction

The rapid digital transformation of sexual and reproductive healthcare has fundamentally reshaped how individuals access information, services, and clinical support. Telemedicine consultations for contraception and abortion counseling, mobile fertility and menstrual-tracking applications, electronic reproductive health records, and virtual prenatal care platforms have expanded access to reproductive health services, particularly for populations facing geographical, social, or legal barriers. These innovations have been widely recognized for improving convenience, continuity of care, and reach within sexual and reproductive health and rights (SRHR).

However, the increasing reliance on digital technologies has also introduced significant cybersecurity vulnerabilities that threaten the integrity, confidentiality, and trustworthiness of reproductive healthcare systems. Sexual and reproductive health data are among the most sensitive categories of personal information, encompassing fertility status, contraceptive use, pregnancy outcomes, abortion-related data, sexual

behavior, and intimate clinical histories. Unauthorized access, data breaches, or misuse of such information can result in serious social, psychological, legal, and health-related consequences, particularly in contexts where reproductive choices are stigmatized or legally contested.

Unlike general healthcare cybersecurity concerns, vulnerabilities in digital reproductive health systems carry distinct ethical and rights-based implications. Compromised reproductive health data can undermine patient autonomy, deter individuals from seeking care, and disproportionately affect marginalized groups such as adolescents, migrants, low-income women, and those living in restrictive legal environments. For these populations, digital reproductive health services often represent the primary or only point of access to care, making robust cybersecurity protections essential for ensuring equity and justice within SRHR delivery.

Despite the centrality of trust, privacy, and autonomy to reproductive healthcare, cybersecurity is frequently treated as a technical or administrative issue rather than a core component of healthcare quality and rights protection. This framing risks overlooking how digital vulnerabilities directly influence clinical safety, patient decision-making, and confidence in reproductive health systems. As digital SRHR services continue to expand globally, particularly in response to public health emergencies and resource constraints, the absence of strong cybersecurity governance poses a growing threat to the sustainability and legitimacy of these services.

This commentary argues that cybersecurity must be recognized as an integral element of sexual and reproductive healthcare integrity rather than a peripheral technical concern. By examining cybersecurity challenges within digital reproductive health services, this paper highlights the ethical, governance, and policy imperatives required to safeguard reproductive health data, protect patient rights, and maintain trust in increasingly digital models of reproductive healthcare delivery.

Relevance of cybersecurity in maintaining the integrity of reproductive healthcare services

The rapid digitalization of sexual and reproductive healthcare services has transformed how individuals access care, information, and clinical support. Teleconsultations for contraception and abortion counseling, mobile fertility tracking applications, electronic reproductive health records, and virtual prenatal follow-ups have expanded access, particularly for populations facing geographical, social, or legal barriers. However, this digital shift has also introduced profound cybersecurity risks that directly threaten the integrity, confidentiality, and trustworthiness of reproductive healthcare systems.

Sexual and reproductive health data are among the most sensitive forms of personal information. They include fertility status, contraceptive use, pregnancy outcomes, abortion history, sexual behavior, and intimate clinical narratives. Breaches involving such data do not merely represent technical failures; they can expose individuals to stigma, discrimination, legal repercussions, and psychological harm. In this context, cybersecurity must be understood not as a peripheral technical issue but as a fundamental component of sexual and reproductive health and rights (SRHR).

This commentary argues that cybersecurity is essential for maintaining the integrity of reproductive healthcare services and safeguarding patient autonomy, dignity, and equity. It focuses specifically on cybersecurity challenges within SRHR-related digital services and highlights ethical, governance, and policy implications relevant to contemporary reproductive healthcare delivery.

Digital transformation and cyber vulnerabilities in reproductive healthcare

Digital reproductive health services have grown rapidly, particularly during and after the COVID-19 pandemic. Telemedicine has enabled remote consultations for contraception, fertility care, prenatal monitoring, and sexual health counseling.

Mobile applications now assist users in tracking menstrual cycles, ovulation, pregnancy milestones, and hormonal symptoms. While these technologies enhance convenience and access, they also expand the attack surface for cyber threats.

Reproductive health platforms frequently collect large volumes of highly granular personal data, often stored on cloud-based servers or transmitted across multiple digital interfaces. Weak encryption, inadequate authentication mechanisms, insecure third-party integrations, and poor regulatory oversight expose these systems to data breaches, unauthorized access, and misuse. In some cases, commercial reproductive health applications monetize user data, further heightening privacy risks.

Unlike general healthcare data breaches, cybersecurity failures in reproductive healthcare can have uniquely severe consequences. Exposure of abortion-related data, fertility struggles, or sexually transmitted infection histories may result in social exclusion, coercion, or legal vulnerability in restrictive jurisdictions. These risks underscore the need for heightened cybersecurity standards tailored specifically to SRHR services.

Cybersecurity as a core component of sexual and reproductive health and rights

Sexual and reproductive health and rights are grounded in principles of bodily autonomy, informed consent, privacy, and freedom from discrimination. Cybersecurity failures directly undermine these principles. When individuals cannot trust that their reproductive health data will remain confidential, they may avoid seeking care, withhold information from providers, or disengage from digital health services altogether.

Marginalized populations—including adolescents, migrants, low-income individuals, and women in restrictive legal environments—are disproportionately affected. These groups are often more reliant on digital reproductive health services while simultaneously lacking access to secure devices, private internet connections, or digital literacy resources. As a result, cybersecurity vulnerabilities exacerbate existing reproductive health inequities.

From a rights-based perspective, protecting reproductive health data is inseparable from protecting reproductive autonomy. Cybersecurity safeguards are therefore essential to ensuring that digital SRHR services empower rather than endanger users.

Trust, integrity, and clinical safety

The integrity of reproductive healthcare services depends on the accuracy, availability, and reliability of digital systems. Cyberattacks that alter clinical records, disrupt teleconsultations, or compromise diagnostic data can directly affect patient safety. Manipulated fertility data, corrupted prenatal records, or interrupted access to telehealth platforms may lead to delayed care, misinformed clinical decisions, or adverse health outcomes.

Equally important is institutional trust. Reproductive healthcare already operates within socially sensitive and politically contested spaces. Cybersecurity breaches can erode public confidence in digital reproductive health initiatives, undermining long-term adoption and sustainability. Trust once lost is difficult to rebuild, particularly among populations already wary of surveillance or discrimination.

Ethical and governance imperatives

Cybersecurity in reproductive healthcare raises critical ethical questions related to consent, accountability, and governance. Patients often consent to digital data collection without fully understanding how their reproductive health information will be stored, shared, or protected. Transparency regarding data practices remains limited across many digital health platforms.

Healthcare institutions and policymakers have an ethical obligation to implement robust cybersecurity frameworks that prioritize patient protection over convenience or cost-saving. This includes adopting strong encryption standards, enforcing access controls, conducting regular security audits, and ensuring that third-party vendors comply with reproductive health–specific privacy requirements. Governance frameworks must also evolve to address cross-border data flows, commercial exploitation of reproductive health

data, and gaps in regulatory oversight. Without explicit cybersecurity governance tailored to SRHR, digital reproductive health systems risk reinforcing surveillance and inequality rather than advancing rights and wellbeing.

Policy and practice implications

Recognizing cybersecurity as integral to reproductive healthcare quality has several implications for policy and practice. First, cybersecurity requirements should be embedded within national and institutional SRHR strategies, rather than treated as optional technical add-ons. Second, reproductive health providers must receive targeted training on digital security risks and patient data protection. Third, patients should be empowered through digital literacy initiatives that promote safe use of telehealth platforms and reproductive health applications.

At the policy level, regulators should establish clear standards governing the collection, storage, and use of reproductive health data, with explicit protections against misuse. Cybersecurity impact assessments should be mandatory for digital reproductive health tools, particularly those serving vulnerable populations.

Conclusion

The digital transformation of reproductive healthcare offers unprecedented opportunities to expand access, autonomy, and continuity of care. However, without robust cybersecurity protections, these same technologies threaten the integrity of sexual and reproductive health services and the rights they are meant to support. Cybersecurity must be understood as a core ethical and structural component of reproductive healthcare delivery.

Safeguarding reproductive health data is essential to maintaining trust, protecting patient dignity, and ensuring equitable access to care in an increasingly digital world. As reproductive healthcare continues to evolve, integrating cybersecurity into SRHR governance is not merely a technical necessity—it is a moral and public health imperative.

Acknowledgments

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025).

References

1. McCoy SI and Packel L. Lessons from early-stage pilot studies to maximize the impact of digital health interventions for sexual and reproductive health. mHealth. 2020; 6:23.
2. Tolu LB, Feyissa GT and Jeldu WG. Guidelines and best practice recommendations on reproductive health services provision amid COVID-19 pandemic: A scoping review. BMC Public Health. 2021; 21:1–10.
3. Chattu VK, Lopes CA, Javed S and Yaya S. Fulfilling the promise of digital health interventions to promote women's sexual, reproductive, and mental health in the aftermath of COVID-19. Reproductive Health. 2021;18(1):112.
4. Hoffman DA. Increasing access to care: Telehealth during COVID-19. Journal of Law and the Biosciences. 2020;7(1): lsaa043.
5. Hood C. Telehealth cybersecurity. In: A Practical Guide to Emergency Telehealth. Oxford University Press; 2021:81–92.
6. Sommestad T, Karlzén H and Hallberg J. A meta-analysis of studies on Protection Motivation Theory and information security behaviour. International Journal of Information Security and Privacy. 2015;9(1):26–46.