ORIGINAL RESEARCH ARTICLE

Data protection compliance risks in Chinese women's health applications: Commercial logic and reproductive privacy

DOI: 10.29063/ajrh2026/v30i21.9

*Haokai Liu and Tian Tan**

Guanghua School of Law, Zhejiang University, Hangzhou Zhejiang 310008, China

***For Correspondence:** Email: *tiamail@zju.edu.cn*

Abstract

This study aimed to examine data protection compliance risks in five Chinese women's health applications covering menstrual management, pregnancy support, and parenting records. This study analyzed privacy policies, information collection and permission lists, third-party disclosures, and simulated testing of user-facing functions to assess reproductive, pregnancy, parenting, and family health data processing in commercial applications. Three compliance gaps were identified. Data for health management functions extended to device and location data, advertising-related services, and third-party technical services, blurring the distinction between necessary data and non-essential commercial or technical data. Authorization for sensitive reproductive, pregnancy, or parenting information was often presented through registration, profile completion, or function activation, limiting separate consent. Users had limited control over advertising, profiling, and third-party technical services. These limitations may affect trust, accurate self-reporting, and equitable access in digital reproductive health services. The findings of this study support application-specific rules, interface review, and privacy-protective design for women's health applications in China, with relevance for African and other digital health markets. *(Afr J Reprod Health 2026; 30 [21]: 113-122).*

Keywords: Women's health applications; Reproductive health data; Digital reproductive health; Data protection compliance; Personal information protection; China

Résumé

Cette étude visait à examiner les risques de non-conformité en matière de protection des données dans cinq applications chinoises de santé féminine couvrant la gestion des menstruations, le suivi de grossesse et le suivi parental. Elle a analysé les politiques de confidentialité, la collecte d'informations et les listes d'autorisation, les divulgations à des tiers et réalisé des tests simulés des fonctionnalités destinées aux utilisatrices afin d'évaluer le traitement des données relatives à la santé reproductive, à la grossesse, à la parentalité et à la famille dans ces applications commerciales. Trois lacunes en matière de conformité ont été identifiées. Les données relatives aux fonctions de gestion de la santé s'étendaient aux données de l'appareil et de la localisation, aux services publicitaires et aux services techniques tiers, brouillant ainsi la distinction entre les données nécessaires et les données commerciales ou techniques non essentielles. L'autorisation d'accès aux informations sensibles relatives à la santé reproductive, à la grossesse ou à la parentalité était souvent présentée lors de l'inscription, du remplissage du profil ou de l'activation d'une fonction, limitant ainsi la possibilité d'un consentement distinct. Les utilisatrices disposaient d'un contrôle limité sur la publicité, le profilage et les services techniques tiers. Ces limitations peuvent affecter la confiance, l'exactitude des déclarations et l'égalité d'accès aux services numériques de santé reproductive. Les résultats de cette étude plaident en faveur de règles spécifiques aux applications, d'une révision des interfaces et d'une conception respectueuse de la vie privée pour les applications de santé féminine en Chine, et sont pertinents pour les marchés africains et autres marchés de la santé numérique. *(Afr J Reprod Health 2026; 30 [21]: 113-122).*

Mots-clés: Applications de santé féminine ; Données sur la santé reproductive ; Santé reproductive numérique ; Conformité à la protection des données ; Protection des informations personnelles ; Chine

Introduction

As mobile health services expand globally, women's health applications have become important digital entry points for menstrual management, preconception guidance, pregnancy support, and parenting records.[1] These services depend on users' continuous input of menstrual cycles, fertility intentions, pregnancy status, parenting records, and family-related information. These data may reveal not only present physical conditions and future fertility plans[2] but also information regarding partners, children, and other family members.[3] If this information is mishandled, disclosed, or

commercialized beyond the reasonable expectations of users, the consequences may extend from personal information rights to workplace discrimination, social stigmatization, and reduced trust in digital health services. Therefore, women's health applications are considered not only health support tools but also digital services that process sensitive reproductive, parenting-related, and family-related information in commercial settings.

Regulatory attention has also shifted to the commercial use of reproductive health data. In 2021, the United States Federal Trade Commission alleged that Flo Health, a period and ovulation tracking application, shared the sensitive health information of users with external analytics and marketing providers despite promising to keep this information private.[4] This case shows how reproductive health applications may generate privacy risks when health support functions, commercial data processing, and third-party technical services are combined within the same digital service.

China provides an important case for examining these concerns. As one of the world's largest mobile internet markets, China has adopted a legal framework, particularly through the Personal Information Protection Law, which distinguishes general personal information from sensitive personal information. The national policy blueprint known as Healthy China 2030 also promotes health digitization and improved access to health services.[5] In commercial women's health applications, the key question is how these legal and policy requirements are reflected in ordinary app interfaces and function settings. Broad privacy terms, bundled authorizations, third-party software development kit (SDK) access, and designs that make refusal costly for users may weaken necessity and data minimization requirements in personal information processing, the requirement of separate consent for processing sensitive personal information, and users' control over subsequent data processing.

Privacy concerns are now a persistent issue in women's health applications and mobile health services.[6] Menstruation tracking applications particularly highlight this issue because menstrual cycle and reproductive data can support health management while being repurposed for advertising, analytics, and other commercial uses that users may not easily understand or control.[7] Studies on privacy policies of Chinese health apps have examined the content of policy texts and possible improvements from the perspective of health information governance.[8] This study focused on how privacy policy disclosures and permission requests are reflected in the functions and interfaces that users encounter under the Personal Information Protection Law of the People's Republic of China. This issue is especially important in cases where reproductive and family health information may be linked to third-party services and commercial uses. This study addresses this issue through policy document analysis, simulated testing of user-facing functions, and application-level evidence from five widely used women's health apps in China.

We first identified the reproductive, pregnancy, parenting, device, and location data disclosed or requested by the sampled applications and assessed the relationship between these data categories and the functions for which they are presented. Subsequently, we analyzed how separate consent and user control options were presented in registration flows, profile completion steps, permission prompts, and privacy settings. On that basis, we determined what the observed practices indicated for reproductive health data governance in China and for other digital health settings, including the African market, where mobile health services are expanding.

Method

Research design

The study used an empirical qualitative design combining policy document analysis with simulated testing of user-facing functions. The publicly available privacy policies, user agreements, platform-disclosed personal information collection lists, permission lists, children's privacy policies where available, and third-party information-sharing or SDK disclosures of each app were examined. These materials were assessed against the rights and processing requirements established by the Personal Information Protection Law of the People's Republic of China and the Civil Code of the People's Republic of China.[9,10]

Simulated testing of user-facing functions referred to researcher-controlled review of functions and interfaces visible to ordinary users. The review covered registration, profile completion, menstrual

or pregnancy status settings, parenting or family data record functions, community interaction, permission prompts, recommendation interfaces, and privacy setting pages. Specifically, it focused on data requests, permission prompts, recommendation settings, and third-party disclosures visible during ordinary app use and did not involve uploading real patient records, pregnancy information, or child health records.

Sample selection and data sources

Five Chinese women's health applications were examined: Meiyou, Dayima, BabyTree, MamaNet Pregnancy, and QinBaby. These applications were selected as information-rich cases with visible market presence in the service scenarios examined in this study. Meiyou and Dayima cover menstrual and women's health management,[11,12] whereas BabyTree, MamaNet Pregnancy, and QinBaby cover pregnancy support, maternal–infant care, parenting records, and family-oriented records.[13] Market reports and public platform materials supported their selection across visible menstrual, pregnancy-support, and parenting service settings. The sample revealed several common service settings in which reproductive, maternal–infant, and family data are processed in Chinese mobile health applications.

Data were collected in mid-November 2025. For each application, we collected and saved publicly available legal documents and user-facing disclosure materials, including full privacy policies, user agreements, platform-disclosed personal information collection lists, permission lists, children's privacy policies where available, and third-party information sharing or SDK disclosures. Using newly registered accounts on Android devices with default system settings, we performed simulated testing of user-facing functions and retained screenshots of registration pages, profile completion steps, permission prompts, privacy setting pages, recommendation settings, and visible third-party sharing or SDK disclosures where available. These procedures examined public documents, disclosed lists, and ordinary user-facing interfaces but did not test server-side processing or actual third-party data transfers. The collected documents, disclosed lists, and screenshots formed the basis for the application-level evidence reported in Table 1.

To ground the legal assessment in observable application practice, the analysis did not classify materials by privacy policy clauses alone. Instead, disclosed data categories were examined in relation to the functions in which they were requested or described, such as menstrual cycle tracking, pregnancy support, parenting records, community interaction, local services, advertising, or account security. This approach helped distinguish the data serving a user-selected health management function from the data mainly connected to personalization, traffic analytics, or commercial service expansion.

Compliance assessment dimensions

The analysis used four qualitative assessment dimensions derived from relevant legal requirements: necessity and data minimization requirements in personal information processing; separate consent for processing sensitive personal information; transparency of third-party provision or sharing of personal information, including SDK involvement; and user control over personalized recommendation and advertising-related processing. The necessity and data minimization dimension examined whether data fields or device permissions had a reasonable connection with user-selected core functions, such as menstrual management, preconception guidance, pregnancy support, or parenting records. The separate consent dimension examined whether the applications provided a clear consent route distinct from general service terms when processing information regarding reproductive health, pregnancy, sexual health, location, or children. The third-party transparency dimension considered whether third-party recipients or service providers, processing purposes, and data categories were disclosed in a user-facing form. The user control dimension assessed whether users could refuse or disable personalized recommendations, advertising-related processing, or profiling-related services in an accessible way while retaining basic health management functions. These dimensions guided the organization of the application-level evidence discussed in Table 1 and the presentation of the results. In the Results section, the first subsection addresses necessity and data minimization, and the second addresses separate consent. The third subsection addresses third-party transparency and user control together because these issues often overlapped in SDK disclosures,

Table 1: Application-level evidence organized based on qualitative assessment dimensions for five Chinese women's health applications

Application	Service functions and data scope reviewed	Technical and third-party disclosures	Consent, transparency, and user control evidence
Meiyou	Period recording, pregnancy or motherhood status, baby records, and artificial intelligence–assisted functions; inputs include menstrual records, pregnancy stage, baby growth stage, BMI, due date, and sexual health records.	Disclosures cover device identifiers, location/network data, application lists, running process and sensor data; permissions or SDKs also involve camera, microphone, storage, Bluetooth, health data, and advertising data.	Personalized services use information related to the menstrual cycle pregnancy or baby growth stage, device, and location. Settings allow closing personalized recommendations or withdrawing permissions. Third-party categories include advertising, monitoring, content, data, and artificial intelligence service providers.
Dayima	Menstrual cycle app context; registration or profile information includes phone number, sex, age, real name, address, email, and personal physiological information.	The privacy agreement discloses device identifiers; operating system information; installed app lists; location/network data; sensors; and SDK/API services for payment, sharing, and advertising.	GPS location is described as sensitive personal information. Refusal affects GPS-based recommendation or location services but not other app functions. The app provides controls for recommendations, programmatic advertising, and system permissions.
BabyTree	Preconception, pregnancy, and parenting functions; stage data include pregnancy/baby's birth status, parental role, baby's sex, baby's birthday, gestational week, expected delivery date, last menstrual period, and menstrual cycle.	Information display and recommendation sections disclose device identifiers, browsing data, search or order information, and stage-related data. Advertising and push SDKs refer to device identifiers, IP addresses, sensors, installed app lists, and profile labels.	The policy distinguishes between basic and extended functions and promises renewed or separate consent for additional functions, non-essential information, and sensitive personal information. It also describes permission pop-ups, third-party sharing, and personalized advertising management.
MamaNet Pregnancy	Preconception, pregnancy, and parenting identity/status; profile-completion and search contexts include birthday, city, identity status, pregnancy stage, baby's age, menstrual records, and search keywords. Child-related functions include photos, cloud albums, and growth records.	Device information includes device identifiers, IP addresses, Wi-Fi/base station/network data, and system or device parameters. The policy also refers to running process information, third-party SDK use, data services, advertising monitoring, statistics, and analytics partners.	Additional function data can be separately accepted or refused, and permissions are requested by pop-ups. Refusal or withdrawal affects related functions but not basic services. Controls include permission management and personalized recommendation or advertising settings.
QinBaby	Baby and pregnancy spaces; baby identity information; cloud album photos, videos, and audio; growth, vaccination, feeding, symptom, sleep, and stool	The privacy policy discloses device identifiers, location/network data, and running process information. Permission and SDK/API disclosures cover camera,	The policy distinguishes basic service information from optional information for extended functions. Settings cover personalized content, personalized advertising, and programmatic advertising; closing

	records; pregnancy functions; and AI assistant for parenting.	microphone, Bluetooth, album/storage, location, smart-device connection, app, sensor, and advertising interaction data.	advertising controls lowers relevance rather than the number of ads. Some child data functions require specific answers.

Notes: This table is descriptive and does not use numerical scores. Evidence follows the qualitative assessment dimensions described in the Methods section. Materials included privacy policies, personal information collection lists, permission lists, third-party sharing or SDK disclosures, children's privacy policies where available, and user-facing observations. SDK, software development kit; API, application programming interface. Device identifiers include IDFA, OAID, Android ID, IMEI, and other similar identifiers. Location/network data include GPS, IP address, and Wi-Fi/WLAN and base-station data.

advertising-related processing, and recommendation settings.

The policy texts, screenshots, and simulated observations were reviewed against the four assessment dimensions. The review produced qualitative consensus observations rather than numerical ratings. The authors compared the materials with the predefined dimensions and discussed items requiring judgment before including the observations in Table 1.

Ethical consideration

This study did not recruit human participants or process real user health records. It relied on publicly available policy documents and user-facing functions accessible through ordinary registered accounts. The authors did not access restricted systems; bypass technical controls; collect personal information from other users; or upload real patient, pregnancy, or child health records. No separate permission from application providers was sought for this analysis of public documents and user-facing interfaces.

Results

The reviewed materials showed three recurring patterns across the five applications. First, health management functions were commonly documented together with device identifiers, location-related data, installed application lists, running process information, personalized recommendations, advertising-related services, and third-party SDK involvement. Second, consent and refusal options for information regarding reproductive health, pregnancy, parenting, and family health were often embedded in registration, profile completion, function entry, or privacy-setting paths rather than presented as clearly separated choices. Third, third-party service disclosures, personalized recommendation settings, and advertising controls often appeared together, with user control mainly provided through opt-out or settings paths. Table 1 organizes the application-level evidence from the examined privacy policies, information collection lists, permission lists, third-party sharing and SDK disclosures, and user-facing observations.

Health management functions and scope of data disclosure

This section addresses the scope of data disclosures associated with health management functions. As shown in Table 1, applications offering menstrual cycle tracking, pregnancy support, or parenting records also disclose data or services linked to local services, e-commerce, advertising-related services, personalized recommendations, and community interaction. These wider services were not consistently separated from the health management functions selected by users. This overlap makes it difficult to distinguish the data needed for a selected health management function from the data connected with broader platform services.

This pattern was most clearly observed in disclosures concerning device identifiers, application list information, running process information, and location-related data. Dayima and QinBaby disclosed multiple device identifiers, including IMEI, MAC address, and Android ID–related information, alongside Wi-Fi, sensor, and location-related categories. Meiyou and MamaNet Pregnancy disclosed data categories related to reproductive, pregnancy, or parenting status while referring to personalized services or recommendation contexts. Several disclosures linked device or technical data to account security, risk control, or service quality, but they did not consistently explain how these data relate to basic menstrual cycle tracking, pregnancy support, or parenting record functions. The relevant evidence in

Table 1 shows that core health functions, extended commercial services, and technical data categories are presented within the same service framework.

Consent and refusal options at registration, profile completion, and function entry

This section addresses how consent routes and refusal options are presented at registration, profile completion, and function entry. The consent-, control-, and transparency-related evidence in Table 1 shows that consent was often linked to registration, profile completion, or entry into particular functions. Consent routes were commonly presented through privacy policies, registration agreements, profile completion steps, or prompts shown when users enter particular functions. BabyTree listed preconception, pregnancy or parenting status, baby's birthday, expected delivery date, last menstrual period, and menstrual cycle information in registration or profile completion contexts. Meiyou listed menstrual information, pregnancy information, pregnancy history, sexual behavior information, or sexual health records in recording, health analysis, and artificial intelligence (AI) assistant contexts. In these cases, general service terms, sensitive information processing, and function activation were presented in closely connected user flows.

Table 1 also shows variation in how refusal options were described across applications and functions. Several policies distinguished between basic and additional functions and stated that refusal to provide information for extended functions would not affect basic services. Reproductive status, pregnancy information, and parenting records also appeared in core service functions. QinBaby linked baby's birthday or expected delivery date to parenting- or pregnancy-related services, including growth assessment, feeding records, vaccination records, pregnancy weight records, prenatal checkup functions, and AI assistant for parenting. These examples show that users may be asked to provide reproductive, pregnancy-related, or parenting-related information at registration, profile completion, or function activation. Therefore, the relevant evidence in Table 1 places consent routes; refusal options; and requests for reproductive, pregnancy-related, or parenting-related information within the same registration, profile completion, and function entry pathways.

Third-party services, personalized recommendations, and user control settings

This section addresses third-party service disclosures, personalized recommendations, and advertising control settings. Third-party sharing lists and SDK disclosures identified providers of advertising, analytics, push notifications, security services, and risk control services. The disclosed data categories included device identifiers, network information, application list information, running process information, location-related data, and advertising identifiers. These technical data categories do not, in themselves, constitute reproductive health information. However, Table 1 shows that they were disclosed in the same service framework as information on menstrual cycles, pregnancy, parenting, or family health.

Meiyou and BabyTree disclosed device identifiers, including advertising-related identifiers, and SDKs or third-party sharing arrangements. MamaNet Pregnancy linked preconception, pregnancy, or parenting status to search and recommendation contexts. QinBaby disclosed opt-out paths for personalized and programmatic advertising recommendations and stated that disabling these settings would reduce advertisement relevance rather than the number of advertisements. The relevant evidence in Table 1 shows information related to reproductive health, pregnancy, parenting, and family alongside advertising, recommendation, and third-party technical services. User control was mainly presented through opt-out or settings paths rather than through separate controls tied to individual advertising, recommendation, or third-party services.

Discussion

Compliance gaps between legal rules and app design

In the five applications examined in this study, the main compliance problem lies in the gap between legal requirements, policy language, and the choices users encounter during ordinary app use.[14] The debate surrounding the Natural Cycles app similarly shows that when fertility management is delivered through app-based algorithmic guidance, regulatory assessment must consider not only formal approval

or clearance status but also marketing claims, user understanding, and the user-facing processes through which reproductive choices are shaped.[15] The Civil Code and the Personal Information Protection Law establish baseline requirements concerning personal information rights and interests, sensitive personal information, necessity and data minimization, separate consent, and the provision of personal information to other personal information processors. Several applications examined in this study also included policy rules on necessity, authorization, refusal to provide information, withdrawal of authorization, and extended functions. The practical effect of these rules depends on how they are reflected in app design and user-facing processes.[16] When menstrual tracking, pregnancy support, and parenting records are offered through app services, they may be combined with community features, e-commerce, local services, advertising delivery, content recommendation, and third-party SDK involvement.[17] Therefore, necessity and data minimization assessment should ask whether each requested data item is needed for the health management function selected by the user and whether non-essential data collection for commercial services or platform operation is clearly separated from that function.

User interfaces and ordinary app use processes further shape the practical effect of necessity and data minimization requirements, as well as the separate consent requirement for processing sensitive personal information.[6] Privacy policies may list data categories, and user agreements may state the scope of authorization, but users usually make practical decisions at registration, profile completion, function entry, permission prompts, or recommendation settings. Information related to menstrual cycle, pregnancy, and parenting; infant images; and family records may appear in the same registration, profile completion, or function use processes as device identifiers, location permissions, search recommendations, or SDK-related services. The legal distinctions between ordinary personal information, sensitive personal information, necessary information, and optional information may not appear to users as clear and separate interface choices. Even after formal notice is provided, users may still face a sequence of profile settings, bundled authorization steps, or a practical trade-off between providing information and losing the value of a function. Therefore, compliance assessment should examine app design and user-facing processes directly. The key questions are whether platforms distinguish basic health management functions from commercialized services; provide separate and explicit consent mechanisms for processing sensitive personal information; and make third-party sharing, recommendation, and advertising practices identifiable and controllable for users. Only under these design conditions can the rights and obligations stated in policy text have practical force in everyday app use.

Trust, accurate self-reporting, and digital health exclusion

Digital reproductive health services depend on sustained use and reasonably accurate self-reporting by users. Cycle tracking, pregnancy reminders, and parenting support usually require users to enter physical status, symptom changes, fertility intentions, and family-related health information over time. When users cannot tell whether such information may be used for recommendation, advertising, community interaction, third-party SDK-related services, or other commercial purposes and cannot see how to limit such use, they may use the service more cautiously or defensively. Defensive use may result in selective recording; delayed entries; vague responses; avoidance of photographs, health histories, or family records; or disabling of functions related to recommendation, advertising, and third-party services. These practices may protect users at the individual level, but they can reduce the data quality on which digital health tools depend. Cycle prediction, pregnancy reminders, parenting advice, and health risk prompts all require relatively accurate and continuous user-entered data. If the underlying data become fragmented, delayed, or inaccurate, the reliability of the service may also decline. Health privacy concerns, perceived surveillance, and the risk of secondary use of reproductive data can affect users' trust in platforms, their willingness to disclose information accurately, and their likelihood of continued service use.[7]

Reproductive and family health information can also have consequences beyond the health service setting, which is why the trust issue is not

limited to individual privacy protection. Fertility intentions, pregnancy status, miscarriage history, infertility treatment, sexual health records, infant images, and child growth records may carry implications for employment evaluation, family relations, social reputation, and gendered stigma.[18] The concern is not only that a platform collects a single data item but also that reproductive or family health information may be reinterpreted and recombined through commercial profiling, advertising delivery, community dissemination, or third-party services. Users with greater privacy literacy, more service alternatives, or lower social exposure may manage these risks through privacy settings, service switching, or selective participation. Women facing employment insecurity, family pressure, stigma, or limited access to health resources may have fewer practical ways to manage these risks; therefore, they may reduce accurate self-reporting or disengage from digital health support. The resulting public health risk may appear as lower data quality, reduced sustained engagement, and reduced participation among socially or medically vulnerable users. For digital reproductive health services, data protection rules are not only tools for the protection of individual rights; they also form part of the conditions for trustworthy health support. Such applications are more likely to sustain reliable data input and user trust when users are able to understand, limit, and control the subsequent use of sensitive reproductive and family-related health information.

Comparative implications for African and other digital health markets

The application-level evidence from the five Chinese applications examined in this study has comparative value because it connects the compliance risks identified above with ordinary app use processes, including registration, function entry, privacy settings, personalized recommendation, and advertising-related services. It shows that, even in a setting with formal personal information protection rules and a large platform economy, health management functions can be closely linked to advertising infrastructure and third-party technical services. Similarly, the privacy enforcement action in the case of Flo Health in the United States indicates that reproductive health data can be connected to external analytics, advertising, and other platform services found outside China.[19] In African and other markets, the value of this evidence lies in the governance pressures that can accompany the expansion of mobile health services across different legal and institutional settings. As applications become convenient, low-cost, and continuous entry points for reproductive health, menstrual records, pregnancy-related information, and parenting data may move beyond health management and become useful for platform operation and commercial use. This concern is especially important in cases where mobile health ecosystems develop faster than the rules, enforcement resources, or oversight mechanisms that govern sensitive data processing.

In African reproductive health settings, these governance questions are closely associated with access. Mobile health applications may help women and adolescents obtain reproductive health information, pregnancy support, menstrual management tools, and entry points for remote consultation, especially in cases where health resources are unevenly distributed, offline services are costly to reach, or reproductive issues carry social stigma.[20] Applications that expand reach also bring questions of privacy, consent, and third-party data flows into reproductive health services. These questions matter in reproductive health contexts wherein privacy, informed consent, dignity, and non-abusive care already shape women's trust in service provision.[21] Early app design is important because broad authorization language, personalized recommendations, advertising SDKs, and third-party analytics can become embedded in interface design, technical arrangements, and commercial contracts before regulatory standards are clearly specified. Therefore, the evidence from this study supports earlier clarification of service boundaries, the requirement of separate consent for processing sensitive personal information, and rules governing third-party sharing and advertising-related infrastructure in digital reproductive health services.[22]

Three governance implications follow. First, protection of reproductive health data should move beyond general privacy policy language toward context-specific standards. Menstrual cycle data, pregnancy intentions, abortion or miscarriage history, sexual health records, and child-related family data require more specific rules on necessity, retention periods, third-party access or sharing, and

the consequences of refusing to provide information than those applicable to ordinary account information. Second, regulatory review should extend beyond privacy policy text to user interfaces and technical infrastructures. Permission prompts, default settings, SDK lists, personalized advertising controls, and the moments at which users are asked to disclose sensitive information shape whether separate consent for processing sensitive personal information can operate as a real choice. Third, privacy by design should be implemented through minimized data retention, local processing, and granular opt-in mechanisms for functions such as cycle prediction, ovulation calculation, pregnancy reminders, and parenting records. For African and other markets, the central concern is to prevent opaque data commercialization structures from becoming embedded while mobile reproductive health services are still expanding.

Limitations

The findings of this study should be interpreted within the scope of the materials and methods used in this study. The sample consisted of five purposively selected women's health applications covering various service settings examined in this study, including menstrual management, pregnancy support, parenting records, and family-related health data, rather than a statistically representative market sample. The materials primarily consisted of publicly available privacy policies, disclosed lists, permission explanations, screenshots, and simulated testing of user-facing functions. These materials allowed us to examine the relationship between policy text, interface design, and application-level evidence; however, this analysis does not amount to technical forensic analysis of server-side processing, actual third-party data flows, or security vulnerabilities. The analysis was grounded in laws and applications operating in the Chinese market; therefore, its implications for African and other markets should be interpreted based on local legal capacity, platform ecosystems, health system conditions, and social norms surrounding reproductive health. The discussion identified plausible public health risks related to accurate self-reporting, sustained use, and digital health exclusion; however, it did not directly measure the behavior of the users of the sampled applications. Future studies may combine policy analysis with technical audits, user interviews, surveys, or cross-jurisdictional comparison to examine the relationship between disclosed data practices, actual data flows, user trust, and service use.

Conclusion

Public disclosures and user-facing designs in the five women's health applications examined in this study revealed that information regarding reproductive health, pregnancy, parenting, and family health was often presented alongside device identifiers, location-related data, personalized recommendations, advertising-related services, and third-party SDK involvement. The relevant data minimization principle is that applications should request and users should be asked to provide only the data needed for the health management function selected by the user. Collection of non-essential data should be minimized. Compliance risks arise when privacy policies and consent clauses provide formal routes for notice and authorization, but app design and ordinary use processes blur the boundary around necessary data collection, weaken the separate consent requirement for processing sensitive personal information, or limit the practical control of users over subsequent data use. In digital reproductive health services, data protection also has a public health dimension because it can shape user trust, accurate self-reporting, sustained service use, and equitable access. Therefore, the evidence from the five applications in this study points to the need for context-specific protection standards, interface and technical review, clearer disclosure of third-party technical services, and privacy-by-design mechanisms. For Chinese, African, and other markets, the broader implication is that mobile reproductive health services should expand without making sensitive reproductive and family-related health information a condition for access.

Funding

This work was financially supported by the Youth Program of Sichuan Medical Law Research Center and China Health Law Society (YF24-Q31).

Authors' contributions

Liu Haokai conceived the article, designed the study, drafted the Chinese manuscript, and reviewed and

revised the English version. Tan Tian contributed to the Chinese draft, prepared the English translation, and participated in manuscript revision. Tan Tian is listed as a co-first author in recognition of his substantial contribution to the preparation and revision of the manuscript.

Data availability

The public policy documents and disclosed lists analysed in this study were publicly accessible at the time of data collection. The authors retained copies of the reviewed public documents and screenshots as part of the research record. These materials are available from the corresponding author on reasonable request, subject to applicable platform terms and privacy considerations.

Conflict of interest

The authors declare no conflict of interest.

References

1. Scatterday A. This is no ovary-action: Femtech apps need stronger regulations to protect data and advance public health goals. North Carolina Journal of Law & Technology 2022;23(4):636-668.
2. Bhatia R. A loophole in the Fourth Amendment: The government's unregulated purchase of intimate health data. Wash L Rev Online. 2024; 98:67-101.
3. Citron DK. A new compact for sexual privacy. Wm & Mary L Rev. 2021; 62:1763-1839.
4. Federal Trade Commission. In the Matter of Flo Health, Inc., a corporation: Complaint. FTC Matter/File No. 192 3133. 2021 Jun 22. Available from: https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf
5. Central Committee of the Communist Party of China; State Council of the People's Republic of China. Healthy China 2030 Planning Outline. 2016. Available from: https://www.gov.cn/zhengce/2016-10/25/content_5124174.htm
6. Fowler LR, Ulrich MR. Femtechnodystopia. Stan L Rev. 2023;75:1233-1313.
7. Gilman ME. Periods for profit and the rise of menstrual surveillance. Colum J Gender & L. 2021;41:100-113.
8. Wang X, Wang JX, Gong BL, Cheng GH, Bao LH. Text analysis and optimization of privacy policies of health apps for health information governance. Information Science. 2024;42(8):174-183.
9. Standing Committee of the National People's Congress. Personal Information Protection Law of the People's Republic of China. 2021. Available from: https://en.spp.gov.cn/2021-12/29/c_948419.htm
10. National People's Congress of the People's Republic of China. Civil Code of the People's Republic of China. 2020. Available from: https://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html
11. Meiyou. Meiyou strategic cooperation with Huawei Cloud to support women's health. 18 March 2024. Available from: https://www.meiyou.com/dongtai/xiangqing?id=MzA1bWVpeW91d2Vic2l0ZQ%3D%3D
12. Women of China. Dayima app promotes digital transformation of the medical and health industry. 14 January 2022. Available from: https://www.womenofchina.com/qt/2022/0114/5655.html
13. MoonFox Data. Insight report on development trends in the maternal and infant industry. 2024. Available from: https://www.moonfox.cn/insight/report/1459
14. Waldman AE. Privacy, practice, and performance. California Law Review 2022;110(4):1221-1280.
15. Tran J. Natural Cycles: When an algorithm digitally mandates your sexual health. SMU Sci & Tech L Rev. 2019; 22:179-213.
16. Baharloo K. Consumer news: Fertility tracking apps, DNA testing, and ... vending machines? Developments in FTC and state protections on certain health information. Loyola Consumer L Rev. 2022; 34:140-153.
17. Elvy SA. The vehicle monitoring and collection technology era. Iowa Law Rev. 2024; 110:43-109.
18. Brown EA. The femtech paradox: How workplace monitoring threatens women's equity. Jurimetrics Journal 2021;61(3):289-329
19. Clark MR. Consumer privacy and the Dobbs disruption. U Mich J L Reform. 2024; 58:1-67.
20. Onukwugha FI, Smith L, Kaseje D, Wafula C, Kaseje M, Orton B, et al. The effectiveness and characteristics of mHealth interventions to increase adolescent's use of sexual and reproductive health services in Sub-Saharan Africa: A systematic review. PLoS One. 2022;17(1):e0261973.
21. Ige WB, Ngcobo WB. Exploring midwives' perceptions of respectful maternity care during childbirth in Lagos State, Nigeria: A qualitative inquiry. Afr J Reprod Health. 2022;26(10):21-30.
22. Ciluvai J, Maheswari U. Social media's impact on adolescent health: Comparative analysis of social media-based interventions for adolescent reproductive health education. Afr J Reprod Health. 2024; 28(3):81-91.