UNIVERSITY OF WOLVERHAMPTON

HERALD COLLEGE KATHMANDU

NetraCare

Professionalism Report

Submitted by: Nabin Pyakurel

Student id: 2408201

Supervisor: Sujan Upreti

Reader: Sarayu Gautam

Date: 2026 / 01 / 23

UNIVERSITY OF WOLVERHAMPTON

Table of Contents

1. Social Aspects

Social impacts refer to the potential ways in which NetraCare will affect access, behaviour and trust in case Nepali users self-screen and provide reports to doctors. There are advantages of improved access and more explicit for patient prioritization. The risks are observed when the results are misinterpreted, where the device constraints are used to advantage some or the clinicians are provided with poor quality reports. Inclusion, safe guidance and realistic expectations should be the primary goals of social design.

1.1. Beneficial impacts

1.1.1. Inclusively and accessibility

NetraCare will be in a position to expand access to individuals who have no simple access to eye clinics because of cost, geographic distance, or even lack of specialists. Further evidence shows that smartphones can be successfully used as a tool of eye screening and education when work processes are planned thoughtfully (Koon-ching, 2022). The app must also be designed to be inclusive to all Nepali users with easy Nepali instructions, big buttons, and easy feedback (e.g., lighting/distance check). Diversity of devices is an issue: inferior cameras and low light may lower the quality of screening and increase the chances of errors (Jin, 2024). Thus, NetraCare is advised to employ input-quality verification and conservative outputs in case of low confidence. The barriers can also be minimized by providing accessibility features (high contrast, readable spacing, screen-reader support, and optional audio guidance) to enable users with low vision or low digital literacy.

1.1.2. Collaborative learning and development

NetraCare has the ability to enhance collaboration where the user concerns are transformed into structured report which can be interpreted by the doctors to be used in triage. The teleophthalmology routes indicate that a remote data and clinician control is capable of enhancing the efficiency of screening (Chokshi, 2024). In case the report includes major findings and uncertainty (not only a single label), clinicians will be able to prescribe the course of action: retesting, routine check-up, or emergency intervention because of red-flag symptoms. Health literacy can also be developed in the app wherein the user is informed of the meaning of every test and that screening is not diagnosis. Community health workers can also use the app in rural communities to assist them in deciding on when a referral is necessary; the app can also assist in providing them with a consistent checklist. By providing explicit opt-in consent, clinician feedback on the usefulness of the reports can be utilized to improve the system and minimize the errors in the future, and no pressure should be exerted on the users to submit data.

1.2. Detrimental impacts

1.2.1. Possible conflict

The primary social risk is that the users will consider the output as a diagnosis. False security may cause a delay in care provision, whereas false alarms may make people anxious and visit more frequently. Smartphone screening in the real-world is sensitive to the behaviour and environment of the user (Koon-ching, 2022), and therefore NetraCare ought to provide results as a guide with precise boundaries. Another cause of conflict is that doctors may be overwhelmed with reports of low quality or frequency that will create workload and negatively affect trust. Teleophthalmology research notes the necessity of a high level of data quality and realistic threshold (Chokshi, 2024). The key features that NetraCare should implement are the labeling of confidence and retesting in case of poor inputs and the provision of urgent-symptom warnings (e.g., sudden loss of vision, severe pain) with an indication that urgent professional treatment is needed.

1.2.2. Moderation challenges

The challenge that NetraCare faces is the issue of quality and misuse management and not social posting. Users can post irrelevant images, do repeat tests wrongly, or attempt to coerce the results to be what they want. Protection of reliability is done by having input-quality checks, clear instructions and restrictions on repetitive submissions. The other trust issue is training AI with user data: ocular media may have a re-identification risk and require well-developed governance (Tom, 2020). NetraCare must submit different consent to model training, permits opt-out with essential features free, and check doctor accounts to eliminate impersonation. Professional credibility and trust in the user is bolstered by audit logs of report access and clear reporting channels of report abuse.

2. Ethical Aspects

The ethical obligations revolve around the autonomy of the user, fairness and transparency. NetraCare makes decisions that can be affected by outputs generated with the help of AI and sensitive health data. Ethical design presupposes the explicit consent, truthful information sharing regarding restrictions, respectful treatment of the user-created content, and no secretive monetization.

2.1. Content ownership

Users are supposed to be regarded as the owners of the screening data and reports. They need to be in a position to see, export, remove and manage sharing of their reports with the doctors. The ownership is of particular concern since NetraCare will be training AI models on user data. The de-identification of ophthalmic data may not necessarily makes it any less sensitive; therefore, secondary usage should be restricted and regulated (Tom, 2020). One such good practice is separate consent: one consent to using the app and one to contributing to training. NetraCare will also need to say what is trained on (raw images or features), minimize the use of the least amount of data possible, and make the option to withdraw consent to future use.

2.2. Data and information privacy

Users are supposed to be informed about the data collected (test values, images/video in case of its use) why it is required, and how it is stored. NetraCare locally stores data in a SQLite3 database minimizing cloud exposure, local storage must have a high level of protection as phones are lost or shared. The privacy settings must be user-friendly: remove examinations, limit access to physicians, and determine what is reported. Raw media must not be stored by default as it should only be stored when the user wants clinicians to look at it. Since ocular data could be re-identifiable, privacy-by-design and minimisation are significant even to so-called anonymous data (Tom, 2020). To fortify the consent process, NetraCare may resort to short, layered screens (summary first, details later) and an apparent Training Data: On/Off switch with the advantages and risks presented in understandable language. In case any export is facilitated later, it must be carried out through encrypted transfer and a record of what was transferred should be recorded.

2.3. No hidden monetization aspect

NetraCare is also free and must not employ any dark patterns that require users to post more, any form of undisclosed tracking, or any data-selling activities. In a case of basic analytics (e.g. crash logs), these should be minimal and aggregated and presented in plain language with opt-out options where feasible. There is also increased responsibility through free access in order to prevent fear-based messages. Findings must be neutral and focused on the subsequent action and not on panic and self-treatment.

2.4. Community engagement

Engagement, in this case, entails the construction of a secure rapport between the users and healthcare providers. The app must direct proper care-seeking and offer red-flags. Fairness, transparency, and accountability are among the outlined requirements of AI ethics in the context of ophthalmology (Chen, 2025). NetraCare is expected to keep track of the performance under various Nepali users and device conditions and report model updates, and give feedback to clinicians and users. Doctor access should be respectful and auditable: the users should be aware of which doctor has accessed a report, and should be capable of disallowing access. Proper instruction of clinicians on how to use NetraCare reports can avoid excessive use of the tool.

3. Legal Aspects

Legal impacts describe how NetraCare must comply with Nepali laws and follow recognised standards for privacy, cyber safety, and intellectual property. Because the system supports doctor access and processes health-related information, documentation (terms, privacy notice, limitation statements) and incident response are key professionalism requirements.

3.1. Nepali laws.

NetraCare being a health-related application that features Nepal only should be able to match the Nepali requirements in terms of privacy and confidentiality. The necessity to secure personal information and communications relies on the Privacy Act, 2075 (Nepal, Government of, 2018). Despite using a local SQLite3 storage, NetraCare needs to safeguard data against un-authorized access, and must offer user controls to view and delete data. There should also be clear limit statements on the site describing that screening is not diagnosis, and how doctor access is done (verification, access logs, and user consent).

3.1.1. Copyright Issues

These can be eye test charts, instructional pictures, or other material that NetraCare may use which can either be copyrighted or licensed. Licensed, permitted, or original materials should be used by the system and sources recorded. The copyright law of Nepal, 2059 (Government of Nepal, 2002) grants copyright on creative works and assists in takedown and enforcement in case of infringement. Working with the rightfully licensed materials will help to avoid litigation and build professional integrity.

3.1.2. Data Protection and Cyber Laws

Some of the responsibilities related to cyber-related issues are secure authentication, safe record management, and incident response process in place. The Electronic Transactions Act, 2063 (Government of Nepal, 2008) of Nepal is a legal framework that regulates against unapproved electronic activities and facilitates safe electronic documents. NetraCare must have access control of doctor accounts, audit trails and simple breach practices (containment, documentation and user notification where applicable). Since the app assists in medical decision-making, the generation of reports and the ability to maintain a strong distinction between automated guidance and clinician judgement should also be documented to decrease the liability and misunderstanding.

3.2. International laws

Although NetraCare may be implemented in Nepal only, international privacy models provide a powerful point of reference and allow making the system future-proof. The GDPR is a popular source of legal processing, transparency and user rights (European Parliament and Council of the European Union, 2016).

3.2.1. Data Protection and Privacy laws.

Trust can be enhanced by adoption of privacy principles like minimisation, purpose limitation, and user rights that will minimize costs of redesign in case the app will be expanded internationally. Since the NetraCare is trained on user data, it is significant to document model versions, consent status and risk assessment. The studies of AI ethics connect the idea of responsible deployment with the responsibility and governance, in particular, when the results can affect the medical decisions (Chen, 2025). NetraCare must establish users, doctors, and developers explicitly, and offer a channel of contact with privacy concerns, and reveal any third-party processing when added in the future.

4. Security Aspects

The security issues include the protection of eye-screening data, doctor-access reports by NetraCare. Local SQLite3 availability allows less exposure to cloud, yet the primary threats become the breach of devices, the use of weak authentication, and the unsecure sharing. In case of using remote services, security-by-design must implement least-privilege access, strong credentials, safe storage and secure APIs.

4.1. No unnecessary display or use of information

NetraCare is advised not to publish superfluous personal details. Only the necessary information to be reviewed by clinicians and used by the user should be displayed in reports and display of identifiers should be controlled by users. The data of local SQLite3 should be encrypted where feasible and not sensitive media should be stored when it is not necessary. An auto locked time out is used and automatic lock on apps to minimize exposure on the shared devices. Exports with consent to training datasets must be kept separately and user-facing information and access should be restricted to reduce harm in case one of the components is breached.

4.2. Password Hashing

In case NetraCare accommodates accounts (particularly of doctors), passwords have to be saved by employing contemporary salted hashing and robust password policies. Multi-factor authentication should be used as a stronger protection in doctor accounts. It limits the rate and provides secure reset flows, which minimize the brute force and takeover risks. The tokens should be short-lived and revocation should be reliable with the help of logout. Access logs aid in the detection of suspicious behaviour and assist in accountability.

4.2. No person data tracking

NetraCare is not supposed to trace users unnecessarily. Eye screening does not necessitate constant location monitoring and this would add to the risk of privacy. In case analytics are required, they must be small, aggregated and published in an easy to understand way. Due to the fact that the training process of AI utilizes data about the user, the system must document the consent status, reduce identifying metadata, and provide an option to opt out without preventing the use of the essential screening capabilities.

4.3. Api protection

In case of the report sharing or doctor portals, all traffic must be done via HTTPS/TLS and under stringent server-side authorization such that users may not compromise the data of other users through identifier guessing. UPS should be checked to eliminate malicious files and injection. The media must not be exposed through open links, but they must be accessed through

authenticated points or time tokens. Basic security testing, dependency updates and secure secrets management are significant. Secure update process should also be implemented in the app to ensure that new model versions or rules cannot be modified. Lastly, an easy reporting of vulnerabilities and the routine examination of third-party libraries can mitigate the long-term risk. These measures are particularly topical since ocular media may be sensitive and re-identifiable (Tom, 2020).

References

Chen, X. Y.-W.-M. (2025). Current status and solutions for AI ethics in ophthalmology: a bibliometric analysis. *npj Digital Medicine, 8*.

Chokshi, T. C. (2024). Advances in teleophthalmology and artificial intelligence for diabetic retinopathy screening: a narrative review. *Annals of Eye Science*.

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Luxembourg: Official Journal of the European Union.

Government of Nepal. (2008). *The Electronic Transactions Act, 2063 (2008).* Kathmandu: Law Commission Nepal.

Jin, K. L. (2024). Integration of smartphone technology and artificial intelligence for advanced ophthalmic care: A systematic review. *Advances in Ophthalmology Practice and Research*, 120–127.

Koon-ching, I. (2022). *The Role of Smartphones in Eyecare: A Systematic Review.* Hong Kong: SAERA – School of Advanced Education, Research and Accreditation.

Nepal, Government of. (2018). *The Privacy Act, 2075 (2018).* Kathmandu: Law Commission Nepal.

Tom, E. K. (2020). Protecting data privacy in the age of AI-enabled ophthalmology. *Translational Vision Science & Technology*.